T S2/5/1

2/5/1
DIALOG(R)File 351:Derwent WPI

013608276
WPI Acc No: 2001-092484/200111
XRPX Acc No: N01-069981
Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not
Patent Assignee: RICOH KK (RICO)
Inventor: KANAI Y; YACHIDA M
Number of Countries: 002 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111	B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113	
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118	
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136	
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138	
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150	
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150	

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1		159	G06F-012/14	
JP 2000339223	A		29	G06F-012/14	
JP 2001005728	A		46	G06F-012/14	
JP 2001147898	A		11	G06F-015/00	
JP 2001154577	A		12	G09C-001/00	
JP 2001209582	A		18	G06F-012/14	
JP 2001209581	A		16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

```
        pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
  ; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06;
  G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?
```

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－339223
（P2000－339223A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ａ	５Ｂ０１７
// Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数８　ＯＬ　（全 29 頁）

(21)出願番号　特願平11－145340

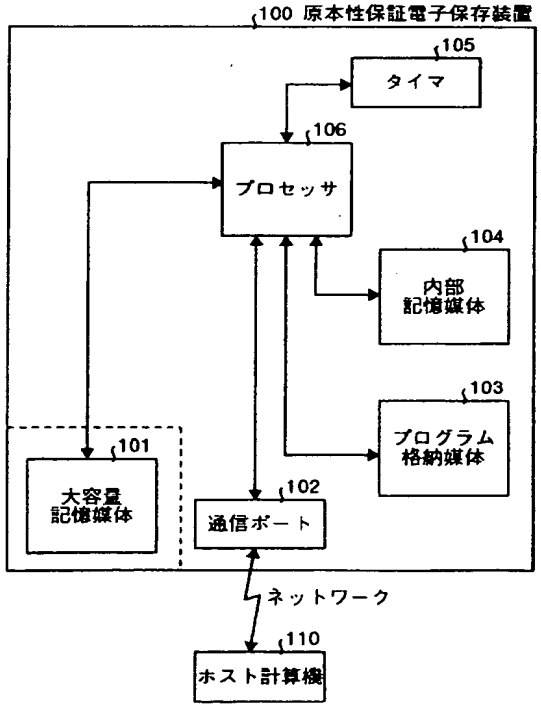
(22)出願日　平成11年５月25日(1999.5.25)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良く行えること。
【解決手段】　複数の版で形成される電子データを一つの原本として識別可能な状態で大容量記憶媒体１０１に保存しておき、プロセッサ１０６がこの大容量記憶媒体１０１の電子データをアクセスするに際しては、原本とそうでないものとでアクセス制御のレベルを変える。



1

【特許請求の範囲】

【請求項１】　所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、

複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、

前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御工程と、

を含んだことを特徴とする原本性保証電子保存方法。

【請求項２】　前記保存工程は、

外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定する第１の改ざん検知情報算定工程と、

前記第１の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、

前記版管理情報作成工程によって作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成するデータ属性情報作成工程と、

前記データ属性情報作成工程によって作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第２の改ざん検知情報算定工程と、

前記第２の改ざん検知情報算定工程によって算定した改ざん検知情報を前記データ属性情報に付与したデータと、保存対象となる電子データとを前記記憶部に記憶する記憶工程と、

を含んだことを特徴とする請求項１に記載の原本性保証電子保存方法。

【請求項３】　前記アクセス制御工程は、

外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、

前記データ属性情報読出工程によって読み出されたデータ属性情報に付与された改ざん検知情報と前記暗号鍵に応答する復号鍵とに基づいて、改ざんの有無を検証する第１の改ざん検証工程と、

前記データ属性情報読出工程によって読み出されたデータ属性情報から読み出し対象となる版の版管理情報を前記記憶部から読み出す版管理情報読出工程と、

前記版管理情報読出工程によって読み出された版管理情報と前記復号鍵とに基づいて、改ざんの有無を検証する第２の改ざん検証工程と、

前記読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供する提供工程と、

を含んだことを特徴とする請求項２に記載の原本性保証電子保存方法。

【請求項４】　外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読み出し工程と、

前記データ属性情報読み出し工程によって読み出されたデータ属性情報と前記復号鍵とに基づいて、改ざんの有無を検証する改ざん検証工程と、

新たな版の電子データに前記暗号鍵を適用して該新たな版の電子データの改ざん検知情報を作成する第１の改ざん検知情報算定工程と、

前記第３の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、

前記版管理情報作成工程によって作成された版管理情報を前記データ属性情報に追加する追加工程と、

前記追加工程によって版管理情報が追加されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第２の改ざん検知情報算定工程と、

前記第２の改ざん検知情報算定工程によって算定された改ざん検知情報を前記データ属性情報に付与したデータと新しい版の電子データとを前記記憶部に記憶する記憶工程と、

からなるバージョンアップ工程をさらに含んだことを特徴とする請求項２または３に記載の原本性保証電子保存方法。

【請求項５】　外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、

前記データ属性情報読出工程によって読み出されたデータ属性情報に前記復号鍵を適用して、該データ属性情報の改ざんの有無を検証する第１の改ざん検証工程と、

前記複製要求で指定された版の電子データを前記記憶部から読み出す電子データ読出工程と、

前記データ属性情報から指定された版の版管理情報を取り出す版管理情報取出工程と、

前記版管理情報取出工程によって取り出された版管理情報に前記復号鍵を適用して、改ざんの有無を検証する第２の改ざん検証工程と、

前記電子データ読出工程によって読み出された指定された版の電子データを指定された複製先に複製する第１の複製工程と、

前記データ属性情報に含まれる属性情報を複写を示す情報に変更する属性情報変更工程と、

前記属性変更工程によって属性情報が変更されたデータ属性情報を指定された複製先に複製する第２の複製工程と、

からなるデータ複製工程をさらに含んだことを特徴とする請求項２、３または４に記載の原本性保証電子保存方

法。

【請求項６】　外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報を前記データ属性情報に含めて管理することを特徴とする請求項１～５のいずれか一つに記載の原本性保証電子保存方法。

【請求項７】　外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することを特徴とする請求項６に記載の原本性保証電子保存方法。

【請求項８】　前記請求項１～７のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法および記録媒体に関し、特に、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる原本性保証電子保存方法および記録媒体に関する。

【０００２】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【０００３】たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－，Medical Imaging Tecnology，Vol.16，No.4，Proceedings of JAMIT AnnualMeeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【０００４】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの従来技術のものは、原本に対する修正または訂正を原本データの追記（差分データ）として取り扱うものであるので、差分が反映された最新または任意の時点の状態

の原本データを取得したいとする外部アプリケーションプログラムの要請に応えることができないという問題がある。

【０００６】すなわち、これらの従来技術は、どこからどこまでが最初に記載された原本データで、どこからが後から追記された原本データであるかを示す情報を原本性保証電子保存装置の外部に提供しないため、かかる外部アプリケーションプログラムの要請に応えるためには、原本データのバージョン管理を外部アプリケーションプログラム側でおこなわなければならなくなる。

【０００７】また、原本性保証電子保存装置によってＣＤ－Ｒなどのリムーバブルメディアに原本データを記録した場合には、このリムーバブルメディアを他のドライブ装置を用いて読み出せることが見読性の観点から見て望ましいが、かかる原本性保証電子保存装置によって記録された原本データは、原本性保証電子保存装置に固有なフォーマットで記録されるため、原本データを作成した外部アプリケーションプログラムがデータを直接解読できないという問題もある。

【０００８】さらに、これらの従来技術では、原本データと該原本データを複製した謄本データとを区別して管理する場合に、原本データの内容全体を謄本データとしていたため、かりに最新の原本データのみが必要であっても、この最新の原本データだけではなく過去の原本データが不要をも含めた内容を全て謄本データに保持せねばならず、記録容量の観点から見て効率的ではないという問題もある。なお、原本データから最新の原本データのみを複製した場合には、この複製データはもはや謄本データではなく、その複製データと原本データの関連は保証されない。

【０００９】これらのことから、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理をいかに効率良くおこなうかが極めて重要な課題となっている。

【００１０】この発明は、上記問題（課題）に鑑みてなされたものであり、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる原本性保証電子保存方法および記録媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明に係る原本性保証電子保存方法は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうア

クセス制御工程と、を含んだことを特徴とする。

【００１２】この請求項１の発明によれば、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる。

【００１３】また、請求項２の発明に係る原本性保証電子保存方法は、前記保存工程は、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定する第１の改ざん検知情報算定工程と、前記第１の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成するデータ属性情報作成工程と、前記データ属性情報作成工程によって作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第２の改ざん検知情報算定工程と、前記第２の改ざん検知情報算定工程によって算定した改ざん検知情報を前記データ属性情報に付与したデータと、保存対象となる電子データとを前記記憶部に記憶する記憶工程と、を含んだことを特徴とする。

【００１４】この請求項２の発明によれば、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成し、作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定し、算定した改ざん検知情報をデータ属性情報に付与したデータと保存対象となる電子データとを記憶部に記憶することとしたので、改ざん検知情報を含むデータ属性情報を電子データとともに記憶することができる。

【００１５】また、請求項３の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に付与された改ざん検知情報と前記暗号鍵に応答する復号鍵とに基づいて、改ざんの有無を検証する第１の改ざん検証工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報から読み出し対象となる版の版管理情報を前記記憶部から読み出す版管理情報読出工程と、前記版管理情報読出工程によって読み出された版管理情報と前記復号鍵とに基づいて、改ざんの有無を検証する第２の改ざん検証工程と、前記読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供する提供工程と、を含んだことを特徴とする。

【００１６】この請求項３の発明によれば、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に付与された改ざん検知情報と暗号鍵に応答する復号鍵とに基づいて改ざんの有無を検証し、読み出されたデータ属性情報から読み出し対象となる版の版管理情報を記憶部から読み出し、読み出された版管理情報と復号鍵とに基づいて改ざんの有無を検証し、読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供することとしたので、改ざんを防止しつつ外部に電子データを提供することができる。

【００１７】また、請求項４の発明に係る原本性保証電子保存方法は、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読み出し工程と、前記データ属性情報読み出し工程によって読み出されたデータ属性情報と前記復号鍵とに基づいて、改ざんの有無を検証する改ざん検証工程と、新たな版の電子データに前記暗号鍵を適用して該新たな版の電子データの改ざん検知情報を作成する第１の改ざん検知情報算定工程と、前記第３の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報を前記データ属性情報に追加する追加工程と、前記追加工程によって版管理情報が追加されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第２の改ざん検知情報算定工程と、前記第２の改ざん検知情報算定工程によって算定された改ざん検知情報を前記データ属性情報に付与したデータと新しい版の電子データとを前記記憶部に記憶する記憶工程と、からなるバージョンアップ工程をさらに含んだことを特徴とする。

【００１８】この請求項４の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出し、読み出されたデータ属性情報と復号鍵とに基づいて改ざんの有無を検証し、新たな版の電子データに暗号鍵を適用して該新たな版の電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報を前記データ属性情報に追加する追加し、追加されたデータ属性情報に暗号鍵を適用して該データ属性情報の改ざん検知情報を算定し、算定された改ざん検知情報をデータ属性情報に付与した

データと新しい版の電子データとを記憶部に記憶することとしたので、改ざんを防止しつつ効率良くバージョンアップをおこなうことができる。

【００１９】また、請求項５の発明に係る原本性保証電子保存方法は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に前記復号鍵を適用して、該データ属性情報の改ざんの有無を検証する第１の改ざん検証工程と、前記複製要求で指定された版の電子データを前記記憶部から読み出す電子データ読出工程と、前記データ属性情報から指定された版の版管理情報を取り出す版管理情報取出工程と、前記版管理情報取出工程によって取り出された版管理情報に前記復号鍵を適用して、改ざんの有無を検証する第２の改ざん検証工程と、前記電子データ読出工程によって読み出された指定された版の電子データを指定された複製先に複製する第１の複製工程と、前記データ属性情報に含まれる属性情報を複写を示す情報に変更する属性情報変更工程と、前記属性変更工程によって属性情報が変更されたデータ属性情報を指定された複製先に複製する第２の複製工程と、からなるデータ複製工程をさらに含んだことを特徴とする。

【００２０】この請求項５の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に復号鍵を適用して、該データ属性情報の改ざんの有無を検証し、複製要求で指定された版の電子データを記憶部から読み出し、データ属性情報から指定された版の版管理情報を取り出し、取り出された版管理情報に復号鍵を適用して改ざんの有無を検証し、指定された版の電子データを指定された複製先に複製し、データ属性情報に含まれる属性情報を複写を示す情報に変更し、変更されたデータ属性情報を指定された複製先に複製することとしたので、改ざんを防止しつつ効率良く電子データを複製することができる。

【００２１】また、請求項６の発明に係る原本性保証電子保存方法は、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報を前記データ属性情報に含めて管理することを特徴とする。

【００２２】この請求項６の発明によれば、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報をデータ属性情報に含めて管理することとしたので、差分データとして電子データを管理する場合であっても効率良く版管理することができる。

【００２３】また、請求項７の発明に係る原本性保証電子保存方法は、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することを特徴とする。

【００２４】この請求項７の発明によれば、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することとしたので、差分データで電子データを管理する場合であっても、さらに効率良く版管理をおこなうことができる。

【００２５】また、請求項８の発明に係る記録媒体は、前記請求項１～７のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１～７の動作をコンピュータによって実現することができる。

【００２６】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００２７】図１は、本実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示すように、この原本性保証電子保存装置１００は、原本となる電子データを記憶し、ネットワークを介してホスト計算機１１０からアクセスされる装置であり、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、タイマ１０５と、プロセッサ１０６とからなる。

【００２８】大容量記憶媒体１０１は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやＣＤ－Ｒなどからなる。通信ポート１０２は、ネットワークを介したホスト計算機との通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００２９】プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００３０】内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。タイマ１０５は、プロセッサ１０６がプログラムの実行時に所得する時刻を計時するタイマである。

【００３１】なお、大容量記憶媒体１０１については、図中に破線で示したように原本性保証電子保存装置１００から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置１００と物理的に一体化し、通信ポート１０２以外からのアクセスを受け付けない耐タンパー性を有する構成にする。ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【００３２】プロセッサ１０６は、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行する制御装置である。

【００３３】具体的には、このプロセッサ１０６は、ユーザから保存要求のあったデータを大容量記憶媒体１０１に保存する際に、あとでデータの改ざんを検出できるようにするために、内部記憶媒体１０４に記憶したプライベートキーを用いて保存するデータにメッセージ認証子を付加する。なお、このメッセージ認証子は、たとえば公開鍵暗号方式を採用した場合には、ディジタル署名として付加するデータに該当する。

【００３４】また、データそのものの不正な抹消を検出するために、大容量記憶媒体１０１に記憶されているデータのリストに対してもメッセージ認証子を付加し、さらにたとえば大容量記憶媒体１０１の状態を過去の状態に戻すような不正なすり替えを検出するために、大容量記憶媒体１０１の媒体識別番号と、その媒体のデータリストに対するメッセージ認証子の対を内部記憶媒体１０４に記憶して管理する。

【００３５】また、データ作成日などを不正に変更することができないように、タイマ１０５から現在時刻を取得し、この時刻をデータの属性として付与するとともに、原本性保証電子保存装置１００内部でオリジナルな電子データである原本データとそのコピーとを区別することができるように、「仮原本」、「原本」および「謄本」といった属性をデータに付与して管理する。たとえば、「原本」という属性が付与されたデータコピーした場合には、このコピーしたデータに「謄本」という属性が付与される。

【００３６】なお、この属性は外部から変更することはできず、また大容量記憶媒体１０１を取り外して外部にてその属性を改ざんしたとしても、この大容量記憶媒体１０１を装置に装着した際に改ざんの有無を検出する。

【００３７】次に、図１に示した原本性保証電子保存装置１００による新規データの保存処理について図２および図３を用いて説明する。図２は、図１に示した原本性保証電子保存装置１００による新規データの保存処理手順を示すフローチャートであり、図３は、この原本性保証電子保存装置１００による新規データの保存処理の概念を説明するための説明図である。

【００３８】図２および図３に示すように、大容量記憶媒体１０１がマウントされている場合には、通信ポート１０２を介してユーザからデータ、データ属性コードおよびデータ名を受け取る（ステップＳ２０１）。具体的には、図３に示す「原本」などがデータ属性コードに該当し、「FileA.doc」などがデータ名に該当する。そして、受け取ったデータ属性コードが「原本」、「仮原本」または「一般」のいずれでもなければ、エラー処理をおこなう。

【００３９】これに対して、このデータ属性コードが「原本」、「仮原本」または「一般」のいずれかであれば、データ属性コードが「一般」であるか否かを判断し（ステップＳ２０２）、「一般」である場合には（ステップＳ２０２肯定）、受け取ったデータを受け取ったデータ名で保存して処理を終了する（ステップＳ２０３）。

【００４０】一方、このデータ属性コードが「一般」でない場合には（ステップＳ２０２否定）、初版としてバージョン属性情報の作成処理をおこなう（ステップＳ２０４）。具体的には、受け取ったデータに対してハッシュ値を計算し、ハッシュ値を装置暗号鍵で暗号化してメッセージ認証子（バージョンＭＡＣ）とし、内部記憶媒体１０４より最新のタイマＩＤを取得し、初版でない場合には、受け取ったバージョンアップモードをデータファイルタイプとし、対象データのバージョン番号、現在時刻、タイマＩＤ、対象データを保存する際のファイル名、データファイルタイプ、対象データのサイズおよびバージョンＭＡＣなどを含むバージョン属性情報を作成するという手順でバージョン属性情報を作成する。なお、図３に示す例では、「Ver.1 1993.3.27 FileA#1.doc 56KB, MAC」からなるバージョン属性情報を作成した場合を示している。

【００４１】その後、この原本性保証電子保存装置１００は、データ属性情報を作成処理する（ステップＳ２０５）。具体的には、内部記憶媒体１０４から最新データ識別番号を取得し、最新データ識別番号を１増加させて内部記憶媒体１０４に記録し、対象データのバージョン属性情報から初版の作成日時情報を取得して作成日時情報を取得して作成日時情報、最終更新日時情報とし、データ属性コード、最新データ識別番号、作成日時情報、最終更新日時情報およびバージョン属性情報などを合わせてデータ属性情報とするという手順でデータ属性情報を作成する。図３に示す例では、「R00012321 原本 1999.3.27 1999.3.27, MAC」というデータ属性情報を作成した場合を示している。

【００４２】その後、大容量記憶媒体１０１から保存データリストファイルを改ざん検知読み出し処理し（ステップＳ２０６）、保存データリストに新たなデータのエ

ントリを追加した後に（ステップＳ２０７）、受け取ったデータ名にバージョン番号を組み込んだファイル名でデータを大容量記憶媒体１０１にファイルとして保存し（ステップＳ２０８）、データ属性情報を改ざん検知保存処理し（ステップＳ２０９）、新しい保存データリストファイルを改ざん検知保存処理した後に（ステップＳ２１０）、保存データリストファイルのメッセージ認証子（リストＭＡＣ）で内部記憶媒体１０４の媒体認証コードリストを更新する（ステップＳ２１１）。

【００４３】具体的には、このデータ属性情報の改ざん検知保存処理では、保存するデータに対してハッシュ値を計算し、ハッシュ値を装置暗号鍵で暗号化し、メッセージ認証子とし、メッセージ認証子とともにデータをファイルとして大容量記憶媒体に保存するという手順の処理をおこなう。

【００４４】次に、大容量記憶媒体１０１のマウント処理について説明する。図４は、図１に示した大容量記憶媒体１０１のマウント処理手順を示すフローチャートである。同図に示すように、まず最初に装着された大容量記憶媒体１０１がフォーマットされているか否かを調べ（ステップＳ４０１）、フォーマットされていない場合には（ステップＳ４０１肯定）、大容量記憶媒体１０１をフォーマットする（ステップＳ４０２）。

【００４５】具体的には、媒体を初期化し、内部記憶媒体１０４から媒体認証コードリストを取得し、媒体認証コードリストから最新の媒体識別番号を取得し、媒体識別番号を１増加させた新しい媒体識別番号を大容量記憶媒体１０１に記録し、内部記憶媒体１０４の媒体認証コードリストに新しい媒体識別番号のエントリを追加する（リストＭＡＣなし）という手順で大容量媒体１０１をフォーマットする。

【００４６】そして、装着された大容量記憶媒体がフォーマット済みの場合（ステップＳ４０１否定）またはステップＳ４０２によるフォーマット処理を終了した場合には、保存データリストファイルを改ざん検知読み出し処理する（ステップＳ４０３）。

【００４７】具体的には、対象ファイルを読み出し、対象ファイルに記録されたメッセージ認証子とデータを分離し、データに対してハッシュ値を計算し、内部記憶媒体１０４から装置暗号鍵を取得し、装置復号鍵でメッセージ認証子を復号して検証用ハッシュ値とし、先のハッシュ値が検証用ハッシュ値と一致しない場合には改ざんされたものと判断する処理をおこなう。

【００４８】そして、改ざんがなされていると判断された場合には（ステップＳ４０４肯定）、エラー処理をおこない（ステップＳ４１０）、改ざんがなされていないと判断された場合には（ステップＳ４０４否定）、大容量記憶媒体１０１から媒体識別番号を取得し（ステップＳ４０５）、この媒体識別番号に該当するメッセージ認証子（リストＭＡＣ）を内部記憶媒体１０４から取得するとともに（ステップＳ４０６）、保存データリストファイルに付与されたメッセージ認証子を取得する（ステップＳ４０７）。

【００４９】そして、両メッセージ認証子が同じであるならば（ステップＳ４０８否定）、認証に成功したものとして正常終了し、両メッセージ認証子が異なる場合には（ステップＳ４０８肯定）、エラー処理する（ステップＳ４１０）。

【００５０】上記一連の処理をおこなうことにより、大容量記憶媒体１０１が取り外し可能な場合に、この大容量記憶媒体１０１のマウント時にその正当性を検証することができる。

【００５１】次に、図１に示した原本性保証電子保存装置１００によるデータ読み出し処理について説明する。図５は、図１に示した原本性保証電子保存装置１００によるデータ読み出し処理手順を示すフローチャートである。

【００５２】同図に示すように、大容量記憶媒体１０１がマウントされた後に、対象データに関連づけられたデータ属性ファイルが存在しない場合には（ステップＳ５０１否定）、対象データファイルを読み出し（ステップＳ５０２）、読み出したデータをユーザに送信して（ステップＳ５１４）、処理を終了する。

【００５３】これに対して、対象データに関連づけられたデータ属性ファイルが存在する場合には（ステップＳ５０１肯定）、大容量記憶媒体１０１の保存データリストファイルから対象データのエントリを取得する（ステップＳ５０３）。なお、対象データのエントリが存在しない場合にはエラー処理をおこなう。

【００５４】そして、このエントリからデータ属性ＭＡＣを取得し（ステップＳ５０４）、大容量記憶媒体１０１から対象データのデータ属性情報ファイルを改ざん検知読み出し処理し（ステップＳ５０５）、改ざんされている場合にはエラー処理をおこなう（ステップＳ５０６）。

【００５５】一方、改ざんされていない場合には、取得したデータ属性情報からデータ属性ＭＡＣを取得し（ステップＳ５０７）、取得したデータ属性ＭＡＣと前のデータ属性ＭＡＣとが一致しない場合には（ステップＳ５０８否定）、エラー処理をおこない（ステップＳ５１５）、両者が一致する場合には（ステップＳ５０８肯定）、大容量記憶媒体１０１から対象データの対象バージョンのデータファイルを読み出す（ステップＳ５０９）。なお、データファイルが存在しない場合には、エラー処理をおこなう。

【００５６】その後、読み出したデータのハッシュ値を計算し（ステップＳ５１０）、データ属性情報から対象バージョンのバージョンＭＡＣを取得するとともに（ステップＳ５１１）、バージョンＭＡＣを装置復号鍵で復号してハッシュ値を取得し（ステップＳ５１２）、両ハ

ッシュ値が異なる場合には（ステップＳ５１３肯定）エラー処理をおこない（ステップＳ５１５）、両ハッシュ値が一致する場合には（ステップＳ５１３否定）、読み出したデータをユーザに送出して（ステップＳ５１４）処理を終了する。

【００５７】上記一連の処理をおこなうことにより、ユーザからデータを受け取ると、対象データの正当性を検証した後に、該当するデータをユーザに送出することができる。

【００５８】次に、図１に示した原本性保証電子保存装置１００による謄本作成処理について説明する。図６は、図１に示した原本性保証電子保存装置１００による謄本作成処理手順を示すフローチャートである。この原本性保証電子保存装置１００では、「原本」の属性を持つデータに対する複製要求を受け取ると、対象データファイルと、それに関連づけられたデータ属性ファイルとを複写し、新たなデータ属性ファイルには「謄本」のデータ属性コードを付加する。

【００５９】具体的には、まず最初に対象データのデータ属性ファイルを改ざん検知読み出し処理をし、読み出したデータ属性情報ファイルからデータ属性コードを取得し、データ属性コードが「原本」であることを確認する。なお、バージョン番号が指定されていない場合には対象バージョンを全バージョンとし、対象バージョン番号が－１である場合には、対象バージョンを最新版とし、対象バージョンが全バージョンでない場合には、完全バージョンから指定されたバージョンまでを対象バージョンとする。

【００６０】そして、図６に示すように、対象データの対象バージョンに対応するバージョンＭＡＣをデータ属性情報から取得し（ステップＳ６０１）、このバージョンＭＡＣを装置復号鍵で復号してバージョンハッシュ値とし（ステップＳ６０２）、対象データの対象バージョンのデータファイルからハッシュ値を計算して（ステップＳ６０３）、ハッシュ値が一致するか否かを確認する（ステップＳ６０４）。

【００６１】その結果、両ハッシュ値が一致しない場合には（ステップＳ６０４否定）、エラー処理をおこなって（ステップＳ６０５）処理を終了し、両ハッシュ値が一致する場合には（ステップＳ６０４肯定）、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ６０６）、保存データリストから対象データのデータ属性ＭＡＣを取得する（ステップＳ６０７）。

【００６２】そして、このデータ属性ＭＡＣが一致しない場合には（ステップＳ６０８否定）エラー処理をおこない（ステップＳ６０５）、データ属性ＭＡＣが一致する場合には（ステップＳ６０８肯定）、作成先が同じ原本性保証電子保存装置であるか否かを調べる（ステップＳ６０９）。

【００６３】そして、同じ装置内である場合には（ステップＳ６０９肯定）、対象データの対象バージョンのデータファイルを作成先にコピーし（ステップＳ６１０）、対象データのデータ属性情報ファイルを作成先のデータ属性情報ファイルとしてコピーし（ステップＳ６１１）、作成先のデータ属性情報ファイルを改ざん検知読み出し処理する（ステップＳ６１２）。

【００６４】そして、読み出したデータ属性情報のデータ属性コードを「謄本」に変更し（ステップＳ６１３）、読み出したデータ属性情報から対象バージョンのバージョン属性情報を取得して（ステップＳ６１４）、バージョン属性情報に含まれるファイル名を新しいファイル名に更新する（ステップＳ６１５）。

【００６５】そして、タイマ１０５から現在時刻を取得し（ステップＳ６１６）、データ属性情報に謄本作成履歴（アカウント名、現在時刻およびタイマＩＤ等）を追加して（ステップＳ６１７）、データ属性情報を改ざん検知保存処理する（ステップＳ６１８）。

【００６６】そして、保存データリストファイルを改ざん検知読み出し処理して（ステップＳ６１９）、保存データリストに作成先データのエントリを追加し（ステップＳ６２０）、新しい保存データリストを改ざん検知保存処理し（ステップＳ６２１）、新しい保存データリストファイルのリストＭＡＣを内部記憶媒体１０４の媒体認証コードリストに記録する（ステップＳ６２２）。

【００６７】これに対して、作成先が同じ装置内でない場合には（ステップＳ６０９否定）、ログイン処理をおこなった後に（ステップＳ６２３）、対象データの対象バージョンのデータファイルを読み出し（ステップＳ６２４）、読み出しデータを作成先装置に謄本作成モードで転送し（ステップＳ６２５）、対象データのデータ属性情報ファイルを改ざん検知読み出し処理する（ステップＳ６２６）。

【００６８】そして、タイマ１０５から現在時刻を取得し（ステップＳ６２７）、データ属性情報に謄本作成履歴を追加し（ステップＳ６２８）、新しいデータ属性情報を作成先の装置に謄本作成モードで転送する（ステップＳ６２９）。

【００６９】次に、図１に示した原本性保証電子保存装置１００のデータ移動処理について説明する。図７および図８は、図１に示した原本性保証電子保存装置１００のデータ移動処理手順を示すフローチャートである。なお、図７は、移動先が同じ装置内である場合を示し、図８は移動先が異なる装置である場合を示している。

【００７０】まず移動先が同じ装置である場合には、まず最初に作成先のデータがすでに存在する場合にはエラー処理をおこない、また対象データにデータ属性情報ファイルが存在しない場合には、対象データのデータファイルを移動先に移動する。

【００７１】そして、図７に示すように、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ

７０１）、読み出した保存データリストから対象データに対応するデータ属性ＭＡＣを取得し（ステップＳ７０２）、対象データのデータ属性情報ファイルからデータ属性ＭＡＣを読み出す（ステップＳ７０３）。

【００７２】そして、対象データの全データファイルを移動先に移動し（ステップＳ７０４）、対象データのデータ属性情報ファイルを移動先に移動した後（ステップＳ７０５）、保存データリスト内の移動したファイルのエントリを更新する（ステップＳ７０６）。

【００７３】そして、新しい保存データリストを改ざん検知保存処理した後に（ステップＳ７０７）、新しい保存データリストファイルのリストＭＡＣで内部記憶媒体１０４の媒体認証コードリストを更新する（ステップＳ７０８）。

【００７４】また、移動先が他の装置である場合には、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ８０１）、移動先の装置にログイン処理する（ステップＳ８０２）。そして、対象データにデータ属性情報ファイルが存在しない場合には（ステップＳ８０３肯定）、対象データのデータファイルを大容量記憶媒体１０１から読み出し（ステップＳ８０４）、読み出したデータを移動モードで転送し（ステップＳ８０５）、対象データのデータファイルを大容量記憶媒体１０１から削除して処理を終了する。

【００７５】これに対して、データ属性ファイルが存在する場合には（ステップＳ８０３否定）、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ８０７）、読み出した保存データリストから対象データに対応するデータ属性ＭＡＣを取得し（ステップＳ８０８）、対象データのデータ属性情報ファイルからデータ属性ＭＡＣを読み出す（ステップＳ８０９）。

【００７６】そして、データ属性ＭＡＣが一致しない場合には（ステップＳ８１０肯定）、対象データのデータ属性情報ファイルを改ざん検知読み出し処理し（ステップＳ８１２）、改ざんされていると判断した場合には（ステップＳ８１３肯定）、エラー処理をおこなって（ステップＳ８１１）処理を終了する。

【００７７】これに対して、改ざんされていない場合には（ステップＳ８１３否定）、対象データの全バージョンについてデータファイルを大容量記憶媒体１０１から読み出し（ステップＳ８１４）、読み出したそれぞれのバージョンについてデータのハッシュ値を計算し（ステップＳ８１５）、データ属性情報から全バージョンについてバージョンＭＡＣを取得し（ステップＳ８１６）、取得したそれぞれのバージョンＭＡＣを装置復号鍵で復号して検証ハッシュ値を取得する（ステップＳ８１７）。

【００７８】そして、対応する検証ハッシュ値と先のハッシュ値のうち、異なるものが存在する場合には（ステップＳ８１８肯定）、エラー処理をおこなって処理を終了し（ステップＳ８１１）、異なるものが存在しない場合には（ステップＳ８１８否定）、タイマ１０５から現在時刻を取得し（ステップＳ８１９）、データ属性情報にデータ移動履歴を追加して（ステップＳ８２０）、新しいデータ属性情報を移動先の装置に移動モードで転送する（ステップＳ８２１）。

【００７９】その後、対象データのデータファイルを全て削除し（ステップＳ８２２）、対象データのデータ属性情報ファイルを削除し（ステップＳ８２３）、保存データリスト内の移動したデータのエントリを削除し（ステップＳ８２４）、新しい保存データリストを改ざん検知保存処理する（ステップＳ８２５）。

【００８０】そして、新しい保存データリストのリストＭＡＣで内部記憶媒体１０４の媒体認証コードリストを更新し（ステップＳ８２６）、作成先装置からログアウト処理をおこなって処理を終了する（ステップＳ８２７）。

【００８１】次に、異なる原本性保証電子保存装置に上記データ移動処理をおこなう場合の移動先の転送受け入れ処理について説明する。図９は、異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の転送受け入れ処理手順を示すフローチャートである。

【００８２】図９に示すように、転送先の原本性保証電子保存装置は、まず最初に転送先データがすでに存在するか否かを確認し（ステップＳ９０１）、すでに存在する場合には（ステップＳ９０１肯定）、エラー処理をおこなって処理を終了する（ステップＳ９０２）。

【００８３】これに対して、転送先データが存在しない場合には（ステップＳ９０１否定）、謄本作成モードであるか否かを確認し（ステップＳ９０３）、謄本作成モードである場合には（ステップＳ９０３肯定）、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ９０４）、受け取ったデータに対してハッシュ値を計算し（ステップＳ９０５）、ハッシュ値を装置暗号鍵で暗号化してバージョンＭＡＣとする（ステップＳ９０６）。

【００８４】そして、受け取ったデータ属性情報の中のバージョンＭＡＣを更新し（ステップＳ９０７）、データ属性情報のデータ属性コードを「謄本」に変更し（ステップＳ９０８）、データ属性情報に謄本作成履歴を追加し（ステップＳ９０９）、新しいデータ属性情報を改ざん検知保存処理する（ステップＳ９１０）。

【００８５】そして、受け取ったデータをデータファイルとして大容量記憶媒体１０１に保存し（ステップＳ９１１）、保存データリストに作成した謄本データのエントリを追加して（ステップＳ９１２）、新しい保存データリストを改ざん検知保存処理し（ステップＳ９１３）、保存データリストファイルのリストＭＡＣで内部記憶媒体１０４の媒体認証コードリストを更新して（ステップＳ９１４）、処理を終了する。

【００８６】一方、ステップＳ９０３において謄本作成モードではなく移動モードであると判断された場合には（ステップＳ９０３否定）、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ２０３）、受け取ったデータに対してハッシュ値を計算し（ステップＳ９１６）、データ属性情報を受け取ったか否かを確認する（ステップＳ９１７）。

【００８７】そして、データ属性情報を受け取った場合には（ステップＳ９１７肯定）、ハッシュ値を装置暗号鍵で暗号化してバージョンＭＡＣとし（ステップＳ９１８）、データ属性情報の中のバージョンＭＡＣを更新して（ステップＳ９１９）、データ属性情報にファイル移動履歴を追加する（ステップＳ９２０）。

【００８８】そして、新しいデータ属性情報を改ざん検知保存処理し（ステップＳ９２１）、受け取ったデータをデータファイルとして大容量記憶媒体１０１に保存して（ステップＳ９２２）、保存データリストに受け取ったデータのエントリを追加する（ステップＳ９２３）。

【００８９】そして、新しい保存データリストを改ざん検知保存処理し（ステップＳ９２４）、保存データリストファイルのリストＭＡＣで内部記憶媒体の媒体認証コードリストを更新して（ステップＳ９２５）、処理を終了する。なお、上記ステップＳ９１７でデータ属性情報を受け取らない場合には（ステップＳ９１７否定）、そのまま処理を終了する。

【００９０】次に、図１に示した原本性保証電子保存装置１００によるデータの削除処理について説明する。図１０は、図１に示した原本性保証電子保存装置１００によるデータの削除処理手順を示すフローチャートである。同図に示すように、まず保存データリストファイルを改ざん検知読み出し処理し（ステップＳ１００１）、対象データに該当するエントリを取得する（ステップＳ１００２）。

【００９１】そして、このエントリが存在しない場合には（ステップＳ１００３否定）、対象データを削除して（ステップＳ１００４）処理を終了し、エントリが存在する場合には（ステップＳ１００３肯定）、データ属性コードが「原本」であるか否かを確認する（ステップＳ１００５）。

【００９２】そして、データ属性コードが「原本」である場合には（ステップＳ１００５肯定）、エラー処理をおこなって処理を終了し（ステップＳ１００６）、「原本」でない場合には（ステップＳ１００５否定）、保存データリストから対象データに該当するエントリを削除し（ステップＳ１００７）、新しい保存データリストを改ざん検知保存処理する（ステップＳ１００８）。

【００９３】そして、保存データリストファイルのリストＭＡＣで内部記憶媒体１０４の媒体認証コードリストを更新した後（ステップＳ１００９）、対象データのデータファイルを削除し（ステップＳ１０１０）、対象データのデータ属性ファイルをも削除して（ステップＳ１０１１）処理を終了する。

【００９４】次に、図１に示した原本性保証電子保存装置１００によるデータ属性コードの変更処理について説明する。データ保存処理において、「仮原本」の属性を持つデータを保存することはできるが、この「仮原本」データは単純にデータ属性コードを「原本」に変更することが可能である。また、「謄本」、「バックアップ仮原本」、「バックアップ原本」および「バックアップ謄本」の属性を持つデータはそれぞれ属性コードを変更することで元のデータを復旧することができる。かかる復旧をおこなうと、図１１に示すように、「謄本」が「原本」に復旧され、「バックアップ仮原本」が「仮原本」に復旧され、「バックアップ原本」が「原本」に復旧され、「バックアップ謄本」が「謄本」に復旧される。なお、かかるデータ属性コードを変更するとこれをデータアクセス履歴として記録することとなる。

【００９５】また、図１２は、図１に示した原本性保証電子保存装置１００によるデータ属性コードの変更処理手順を示すフローチャートである。同図に示すように、まず最初に保存データリストを改ざん検知読み出し処理し（ステップＳ１２０１）、保存データリストから対象データに該当するエントリを取得したならば（ステップＳ１２０２）、エントリから現属性コードを取得する（ステップＳ１２０３）。

【００９６】そして、新データ属性コードが「仮原本」であり（ステップＳ１２０４肯定）、現データ属性コードが「バックアップ仮原本」である場合には（ステップＳ１２０５肯定）、データ属性情報のデータ属性コードを「仮原本」に変更する（ステップＳ１２０６）。なお、ステップＳ１２０５で現データ属性コードが「バックアップ仮原本」でない場合には（ステップＳ１２０５）、エラー処理をおこなって処理を終了する（ステップＳ１２１９）。

【００９７】また、新データ属性コードが「仮原本」でない場合には（ステップＳ１２０４否定）、この新データ属性コードが「原本」であるか否かを調べ（ステップＳ１２０７）、この新データ属性コードが「原本」である場合には（ステップＳ１２０７肯定）、現データ属性コードが「バックアップ仮原本」または「仮原本」であか否かを調べ（ステップＳ１２０８）、「バックアップ仮原本」または「仮原本」である場合には（ステップＳ１２０８肯定）、データ属性情報のデータ属性コードを「原本」に変更する（ステップＳ１２０９）。なお、ステップＳ１２０８で現データ属性コードが「バックアップ原本」または「仮原本」でない場合には（ステップＳ１２０８否定）、エラー処理をおこなって処理を終了する（ステップＳ１２１９）。

【００９８】また、新データ属性コードが「原本」でない場合には（ステップＳ１２０７否定）、この新データ

属性コードが「謄本」であるか否かを調べ（ステップＳ１２１０）、この新データ属性コードが「謄本」である場合には（ステップＳ１２１０肯定）、現データ属性コードが「バックアップ謄本」であか否かを調べ（ステップＳ１２１１）、「バックアップ謄本」である場合には（ステップＳ１２１１肯定）、データ属性情報のデータ属性コードを「謄本」に変更する（ステップＳ１２１２）。なお、ステップＳ１２１１で現データ属性コードが「バックアップ謄本」でない場合には（ステップＳ１２１１否定）、エラー処理をおこなって処理を終了する（ステップＳ１２１９）。

【００９９】そして、これらの変更を終えたならば、タイマ１０５から現在時刻を取得し（ステップＳ１２１３）、データ属性情報にデータ属性コード変更履歴を追加して（ステップＳ１２１４）、新しいデータ属性情報を改ざん検知保存処理する（ステップＳ１２１５）。

【０１００】その後、保存データリストの対象データに該当するエントリについて内容を更新し（ステップＳ１２１６）、新しい保存データリストを改ざん検知保存処理して（ステップＳ１２１７）、保存データリストファイルのリストＭＡＣで内部記憶媒体１０４の媒体認証コードリストを更新して（ステップＳ１２１８）、処理を終了する。

【０１０１】次に、図１に示した原本性保証電子保存装置１００によるデータのバージョンアップ処理について説明する。このデータバージョンアップ処理では、「原本」および「仮原本」のデータ属性コードを持つデータに対しては編集を許可しないが、バージョンアップについては許可することとしている。このように、バージョンアップのみを許可することにより、以前のデータが失われず、電子データの編集履歴が分かるため、その証明力が高まることになる。

【０１０２】また、この原本性保証電子保存装置１００では、「謄本」およびバックアップのデータについては、追記や編集を許可しない。その理由は、データの訂正や修正は、原本に対して施すべきものであり、コピーやバックアップに対して施すべきものではないからである。

【０１０３】また、新しいバージョンのデータ管理の仕方としては、新しいバージョンの内容を完全に記録する方式と、前バージョンとの差分のみを記録する方式とを選択できることとしている。なお、この差分のみを記録する差分モードでは、差分データを外部から渡すこととする。

【０１０４】図１３は、図１に示した原本性保証電子保存装置１００によるデータのバージョンアップ処理手順を示すフローチャートであり、図１４は、この原本性保証電子保存装置１００によるデータのバージョンアップ処理の概念を説明するための説明図である。

【０１０５】図１３および図１４に示すように、大容量記憶媒体１０１がマウントされている場合には、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ１３０１）、読み出した保存データリストから対象データのエントリを取得する（ステップＳ１３０２）。

【０１０６】そして、エントリの中からデータ属性ＭＡＣを取得するとともに（ステップＳ１３０３）、対象データに対応したデータ属性情報ファイルからデータ属性ＭＡＣを取得し（ステップＳ１３０４）、両属性ＭＡＣが一致するか否かを確認する（ステップＳ１３０５）。

【０１０７】そして、両属性ＭＡＣが一致しない場合には（ステップＳ１３０５否定）、エラー処理をおこなって（ステップＳ１３１７）処理を終了し、両属性ＭＡＣが一致する場合には（ステップＳ１３０５肯定）、対象データに対応したデータ属性情報ファイルを改ざん検知読み出し処理する（ステップＳ１３０６）。

【０１０８】そして、読み出したデータ属性情報から最新バージョン番号を取得し（ステップＳ１３０７）、最新バージョン番号に１を加えて現バージョン番号とし（ステップＳ１３０８）、外部から受け取ったデータをもとに現バージョンのバージョン属性情報作成処理をおこなう（ステップＳ１３０９）。たとえば、図１４に示す例では、「Ver.2 1999.3.29 File#2.doc 102KB MAC」というバージョン２（Ver.2）のバージョン属性情報が作成される。

【０１０９】そして、現バージョンのバージョン属性情報をもとにデータ属性情報更新処理をおこなう（ステップＳ１３１０）。具体的には、新しいバージョン属性情報から作成日時情報を取得して最終更新日時情報とし、データ属性情報の最終更新日時情報を新しい最終更新日時情報に更新し、データ属性情報に新しいバージョン属性情報を追加して新しいデータ属性情報とする。たとえば、図１４に示す例では、「R00012321 原本 1999.3.27 1999.3.29 Ver.1 Ver.2 MAC」というデータ属性情報を作成する場合を示している。

【０１１０】そして、大容量記憶媒体１０１から保存データリストファイルを改ざん検知読み出し処理し（ステップＳ１３１１）、保存データリストから対象データに該当するエントリの内容を新しいデータ属性情報をもとに更新する（ステップＳ１３１２）。

【０１１１】そして、対象データのデータ名にバージョン番号を組み込んだファイル名でデータを大容量記憶媒体１０１にファイルとして保存し（ステップＳ１３１３）、新しいデータ属性情報を改ざん検知保存処理するとともに（ステップＳ１３１４）、新しい保存データリストを改ざん検知保存処理して（ステップＳ１３１５）、保存データリストファイルのメッセージ認証子（リストＭＡＣ）で内部記憶媒体１０４の媒体認証コードリストを更新して（ステップＳ１３１６）処理を終了する。

【０１１２】次に、図１に示した原本性保証電子保存装置１００によるデータの編集処理について説明する。この原本性保証電子保存装置１００では、「仮原本」および「原本」のデータについては修正履歴を残すことで証明力を高めるために、データに対する編集要求を拒否し、また「謄本」やバックアップは、本来編集すべき対象ではないので、同様に編集要求を拒否する。このため、結果的に「一般」のデータのみが編集可能となる。

【０１１３】図１５は、図１に示した原本性保証電子保存装置１００によるデータの編集処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体１０１がマウントされている場合には、保存データリストファイルを改ざん検知読み出し処理し（ステップＳ１５０１）、保存データリストから対象データに該当するエントリを取得する（ステップＳ１５０２）。

【０１１４】ここで、このエントリを取得できた場合には（ステップＳ１５０３肯定）、エラー処理をおこなって処理を終了し（ステップＳ１５０５）、エントリを取得できない場合には（ステップＳ１５０３否定）、対象データのデータファイルの編集を許容する（ステップＳ１５０４）。

【０１１５】次に、図１に示した原本性保証電子保存装置１００へのクライアント（ホスト計算機１１０）からのログイン処理について説明する。この原本性保証電子保存装置１００にデータを保存したりデータを読み出す前に、クライアントは原本性保証電子保存装置１００にログインしなければならない。

【０１１６】このログイン処理としては、従来から知られているＩＣカードを用いる技術を採用することもできるが、本実施の形態では、パスワードによる一般的なチャレンジ　レスポンス認証処理をおこなっている。なお、この原本性保証電子保存装置１００は、内部記録媒体１０４のアカウント管理テーブルにあらかじめアカウント名とパスワードを記憶しており、外部システムがアクセスする場合には、外部システム用のアカウント名を使用し、原本の移動やコピーをするために他の原本性保証電子保存装置にログインする際には、原本性保証電子保存装置用のアカウントを使用することとする。

【０１１７】図１６は、図１に示した原本性保証電子保存装置１００へのクライアントからのログイン処理手順を示すフローチャートである。同図に示すように、クライアントがアカウント名とログイン要求を送信し（ステップＳ１６０１）、原本性保証電子保存装置１００が、このアカウント名とログイン要求を受信したならば（ステップＳ１６０２）、内部記録媒体１０４からアカウント管理テーブルを取得する（ステップＳ１６０３）。

【０１１８】そして、クライアントがアカウント名とパスワードを送信すると（ステップＳ１６０４）、原本性保証電子保存装置１００では、アカウント管理テーブルから該当するパスワードを取得し（ステップＳ１６０５）、該当するパスワードが存在しない場合には（ステップＳ１６０６肯定）、エラー処理をおこなって処理を終了する（ステップＳ１６０７）。

【０１１９】これに対して該当するパスワードが存在する場合には（ステップＳ１６０６否定）、乱数を生成してクライアントに送信する（ステップＳ１６０８～Ｓ１６０９）とともに、乱数とパスワードを合わせたものに対してハッシュ値を計算する（ステップＳ１６１０）。

【０１２０】一方、クライアントがこの乱数を受信したならば（ステップＳ１６１１）、乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップＳ１６１２）、計算したハッシュ値を送信する（ステップＳ１６１３）。

【０１２１】そして、原本性保証電子保存装置１００が、このハッシュ値を受信したならば（ステップＳ１６１４）、両ハッシュ値を比較して両者が一致する場合には（ステップＳ１６１５肯定）、成功した終了コードを送信し（ステップＳ１６１６）、両者が一致しない場合には（ステップＳ１６１５否定）、エラー処理をおこなう（ステップＳ１６１８）。そして、クライアントがこの終了コードを受信（ステップＳ１６１７）した時点でログイン処理を終了する。なお、ステップＳ１６０７およびＳ１６１８のエラー処理時には、エラーを示す旨の終了コードをクライアントに送信する。

【０１２２】次に、図１に示した原本性保証電子保存装置１００による日時の管理について説明する。この原本性保証電子保存装置１００では、データアクセス履歴などに記録する日時は装置内部のタイマ１０５から取得するが、このタイマ１０５は設定変更が可能であるため、タイマ１０５を不正に変更することによりデータアクセス日時を偽ることが可能となる。

【０１２３】このため、本実施の形態では、タイマ１０５の設定をおこなうと図１７（ａ）に示すように、タイマ設定履歴を自動的に内部記憶媒体１０４に記憶するよう構成している。

【０１２４】ここで、タイマＩＤは、装置内部で自動的に付与されるシーケンシャルな番号であり、タイマの設定を変更する都度番号が増える。また、データアクセス履歴に含まれる日時情報にはタイマＩＤも含まれる。

【０１２５】同図に示す場合に、タイマＩＤ＝３において不正に日付を１月ずらし、その後タイマＩＤ＝４で日付を戻していることが分かるため、データアクセス履歴の日時にタイマＩＤ＝３の履歴が付されているデータは、不正に日時を偽ろうとした可能性があることが判明する。

【０１２６】また、原本性保証電子保存装置１００から他の原本性保証電子保存装置へデータを移動したりコピーする場合にも、データアクセス履歴の日時に不都合が生じないようにするために、図１７（ｂ）に示すデータアクセス履歴をデータ属性情報に取り込む。なお、この

データアクセス履歴は、データ情報ファイルに記憶する。具体的には、同図に示す例では、移動先の原本性保証電子保存装置R010-0001055の日時19990217 10:13:43 ＩＤ＝２が、移動元の原本性保証電子保存装置R010-0001032の日時19990217 10:10:21 ＩＤ＝３に相当することが分かるため、移動したデータに不正が見つかった場合には、原本性保証電子保存装置をまたいで履歴を辿ることができる。

【０１２７】次に、図１に示した原本性保証電子保存装置１００が用いる保存データリストファイル、データ属性情報ファイル、バージョン属性情報、媒体認証コードリスト、アカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例について図１８および図１９を用いて説明する。

【０１２８】図１８（ａ）は、原本性保証電子保存装置１００が用いる保存データリストファイルの一例を示す図であり、同図に示すように、この保存データリストファイルは、メッセージ認証子（リストＭＡＣ）と各リストエントリからなる。なお、ここで言う原本化とは、属性コードを「仮原本」から「原本」に変更することを意味する。そして、最初のリストＭＡＣを除いた部分が改ざん検知読み出し処理した際の保存データリストとなる。

【０１２９】図１８（ｂ）は、原本性保証電子保存装置１００が用いるデータ属性情報ファイルの一例を示す図であり、同図に示すように、このデータ属性情報ファイルは、メッセージ認証子（リストＭＡＣ）と属性管理データとからなる。そして、最初のデータ属性ＭＡＣを除いた部分が改ざん検知読み出し処理した際のデータ属性情報となる。また、データ識別番号は、原本性保証電子保存装置識別番号（たとえば、R0010123）と、最新データ識別番号（たとえば、00000021）とをつなげたもの（R0010123-00000021）となる。

【０１３０】図１８（ｃ）は、原本性保証電子保存装置１００が用いるバージョン属性情報の一例を示す図であり、同図に示すように、このバージョン属性情報は、メッセージ認証子（リストＭＡＣ）と、バージョン管理データと、各アクセス履歴とからなる。

【０１３１】図１９（ａ）は、原本性保証電子保存装置１００が用いる媒体認証リストコードの一例を示す図であり、同図に示すように、この媒体認証リストコードは、媒体識別番号およびメッセージ認証子（リストＭＡＣ）からなる複数の認証コードエントリにより形成される。

【０１３２】図１９（ｂ）は、原本性保証電子保存装置１００が用いるアカウント管理リストの一例を示す図であり、同図に示すように、このアカウント管理リストは、アカウント名およびパスワードからなる各アカウントエントリからなる。なお、このアカウント管理リストは、任意の数のアカウントが登録できるような構造としているが、最初から存在するクライアント用のアカウントや、原本性保証電子保存装置用のアカウントについては図示省略している。

【０１３３】図１９（ｃ）は、原本性保証電子保存装置１００が用いる日時情報の内容を示す図であり、同図に示すように、この日時情報は、「年」、「月」、「日」、「時」、「分」、「秒」および「タイマＩＤ」からなる。

【０１３４】図１９（ｄ）は、原本性保証電子保存装置１００が用いるタイマ設定履歴ファイルの内容を示す図であり、同図に示すように、このタイマ設定履歴ファイルは、設定前の日時情報、設定後の日時情報およびアカウント名からなる各タイマ設定履歴からなる。

【０１３５】

【発明の効果】以上説明したように、請求項１の発明によれば、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる。

【０１３６】また、請求項２の発明によれば、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成し、作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定し、算定した改ざん検知情報をデータ属性情報に付与したデータと保存対象となる電子データとを記憶部に記憶することとしたので、改ざん検知情報を含むデータ属性情報を電子データとともに記憶することができる。

【０１３７】また、請求項３の発明によれば、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に付与された改ざん検知情報と暗号鍵に応答する復号鍵とに基づいて改ざんの有無を検証し、読み出されたデータ属性情報から読み出し対象となる版の版管理情報を記憶部から読み出し、読み出された版管理情報と復号鍵とに基づいて改ざんの有無を検証し、読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供することとしたので、改ざんを防止しつつ外部に電子データを提供することができる。

【０１３８】また、請求項４の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出

し、読み出されたデータ属性情報と復号鍵とに基づいて改ざんの有無を検証し、新たな版の電子データに暗号鍵を適用して該新たな版の電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報を前記データ属性情報に追加する追加し、追加されたデータ属性情報に暗号鍵を適用して該データ属性情報の改ざん検知情報を算定し、算定された改ざん検知情報をデータ属性情報に付与したデータと新しい版の電子データとを記憶部に記憶することとしたので、改ざんを防止しつつ効率良くバージョンアップをおこなうことができる。

【０１３９】また、請求項５の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に復号鍵を適用して、該データ属性情報の改ざんの有無を検証し、複製要求で指定された版の電子データを記憶部から読み出し、データ属性情報から指定された版の版管理情報を取り出し、取り出された版管理情報に復号鍵を適用して改ざんの有無を検証し、指定された版の電子データを指定された複製先に複製し、データ属性情報に含まれる属性情報を複写を示す情報に変更し、変更されたデータ属性情報を指定された複製先に複製することとしたので、改ざんを防止しつつ効率良く電子データを複製することができる。

【０１４０】また、請求項６の発明によれば、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報をデータ属性情報に含めて管理することとしたので、差分データとして電子データを管理する場合であっても効率良く版管理することができる。

【０１４１】また、請求項７の発明によれば、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することとしたので、差分データで電子データを管理する場合であっても、さらに効率良く版管理をおこなうことができる。

【０１４２】また、請求項８の発明に係る記録媒体は、前記請求項１～７のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１～７の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図２】図１に示した原本性保証電子保存装置による新規データの保存処理手順を示すフローチャートである。

【図３】図１に示した原本性保証電子保存装置による新規データの保存処理の概念を説明するための説明図である。

【図４】図１に示した大容量記憶媒体のマウント処理手順を示すフローチャートである。

【図５】図１に示した原本性保証電子保存装置によるデータ読み出し処理手順を示すフローチャートである。

【図６】図１に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャートである。

【図７】図１に示した原本性保証電子保存装置のデータ移動処理手順（移動先が同じ装置内である場合）を示すフローチャートである。

【図８】図１に示した原本性保証電子保存装置のデータ移動処理手順（移動先が他の装置内である場合）を示すフローチャートである。

【図９】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の転送受け入れ処理手順を示すフローチャートである。

【図１０】図１に示した原本性保証電子保存装置によるデータの削除処理手順を示すフローチャートである。

【図１１】図１に示した原本性保証電子保存装置によるデータ属性コードの変更態様を示す説明図である。

【図１２】図１に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャートである。

【図１３】図１に示した原本性保証電子保存装置によるデータのバージョンアップ処理手順を示すフローチャートである。

【図１４】図１に示す原本性保証電子保存装置によるデータのバージョンアップ処理の概念を説明するための説明図である。

【図１５】図１に示した原本性保証電子保存装置によるデータの編集処理手順を示すフローチャートである。

【図１６】図１に示した原本性保証電子保存装置へのクライアントからのログイン処理手順を示すフローチャートである。

【図１７】図１に示した原本性保証電子保存装置が用いるタイマ設定履歴およびアクセス履歴の一例を示す図である。

【図１８】図１に示した原本性保証電子保存装置が用いる保存データリストファイル、データ属性情報ファイルおよびバージョン属性情報の一例を示す説明図である。

【図１９】図１に示した原本性保証電子保存装置が用いる媒体認証コードリスト、アカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例を示す説明図である。

【符号の説明】

１００　原本性保証電子保存装置
１０１　大容量記憶媒体
１０２　通信ポート
１０３　プログラム格納媒体

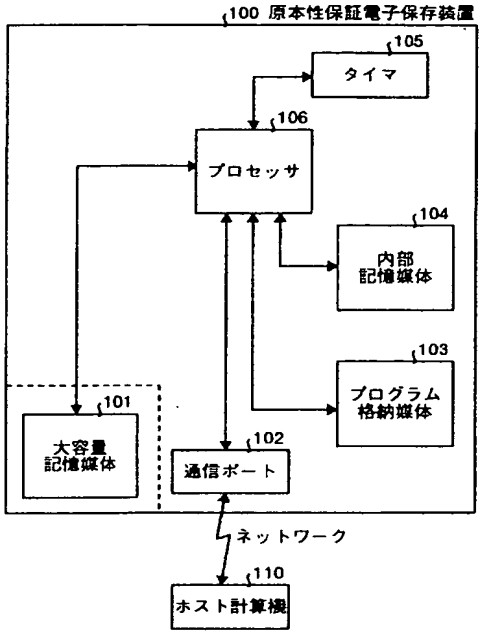
27

１０４　内部記録媒体
１０５　タイマ

28

１０６　プロセッサ
１１０　ホスト計算機

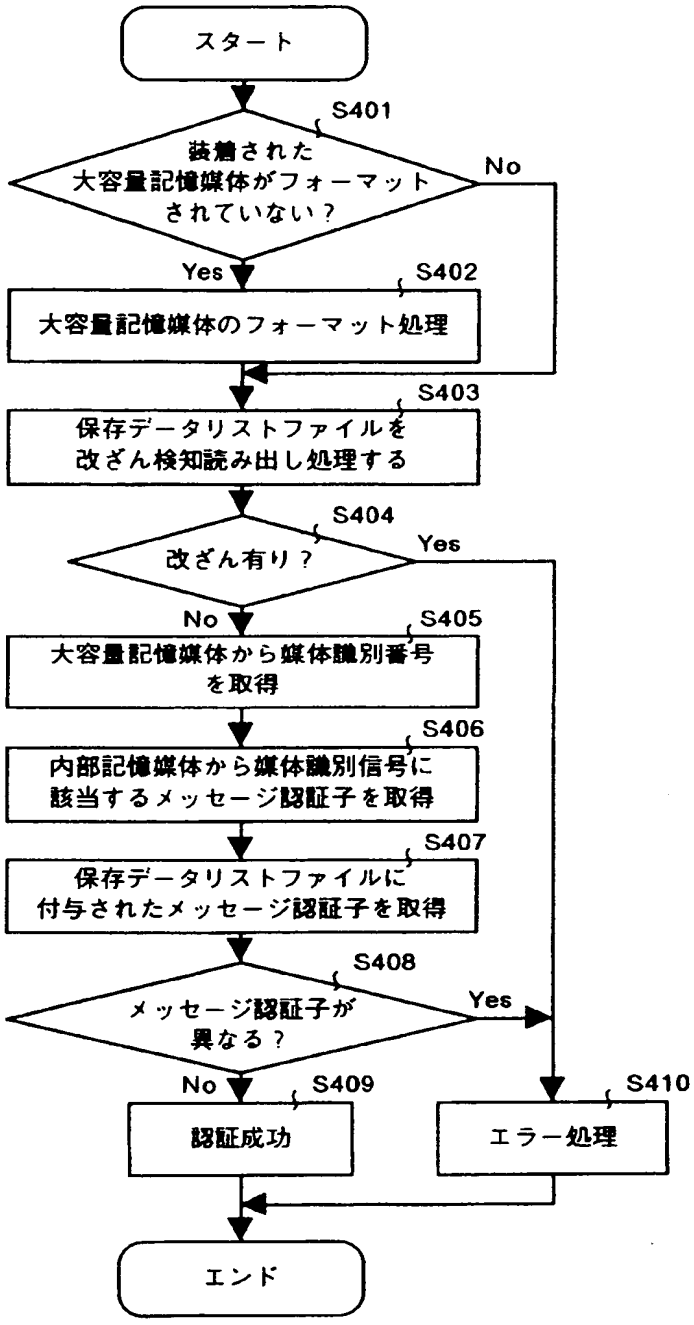
【図１】



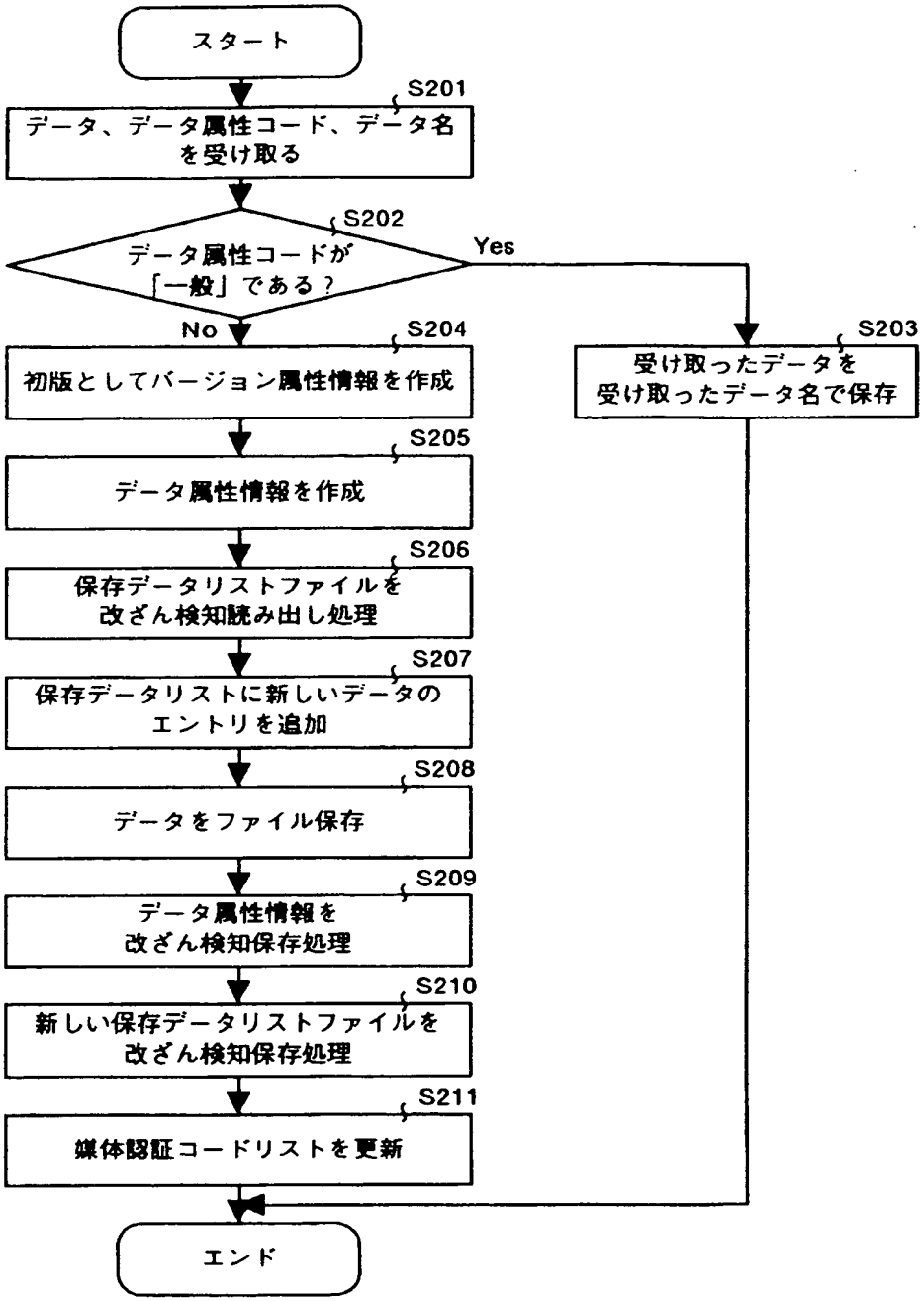
【図１１】

復旧前	復旧後
謄本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ謄本	謄本

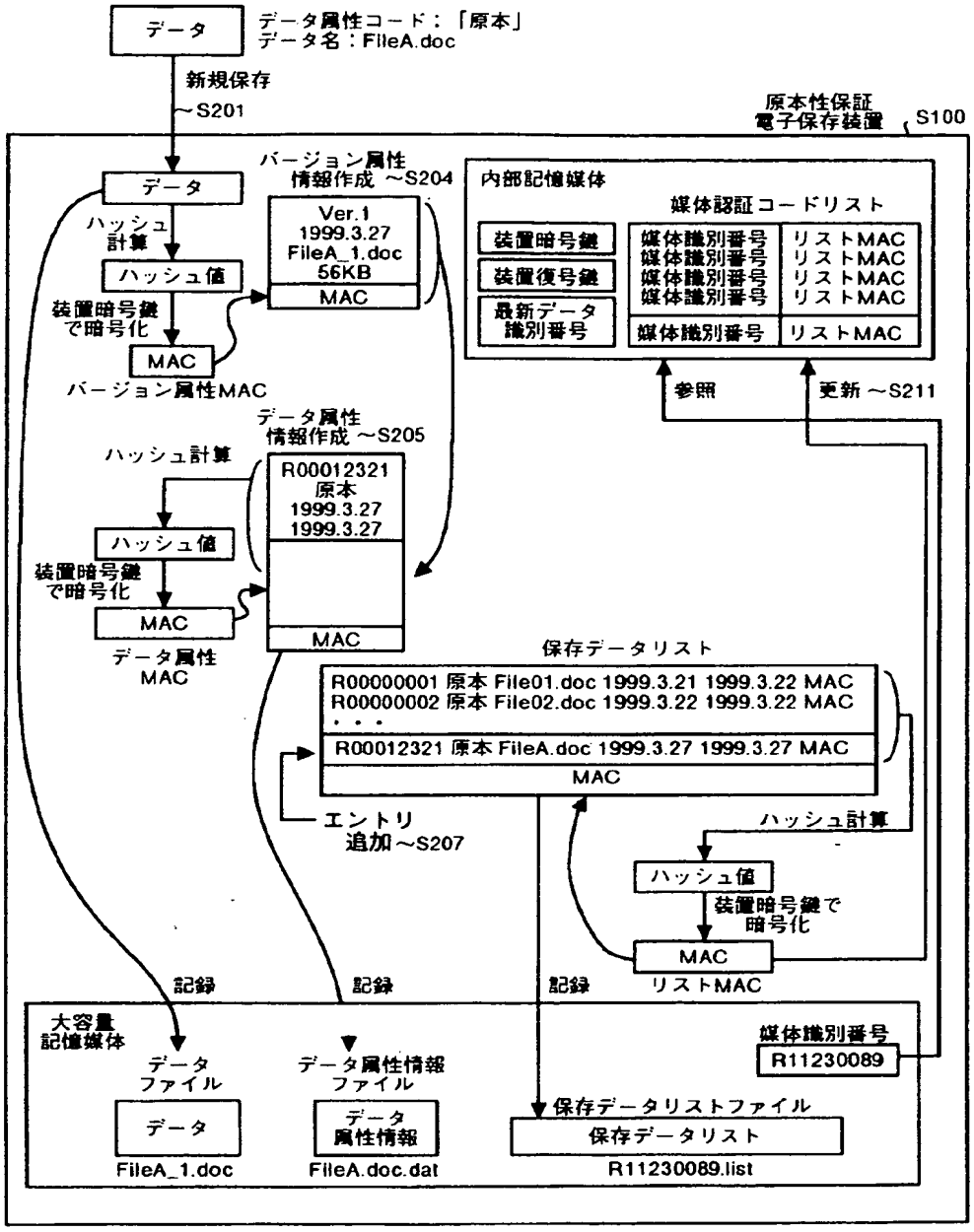
【図４】



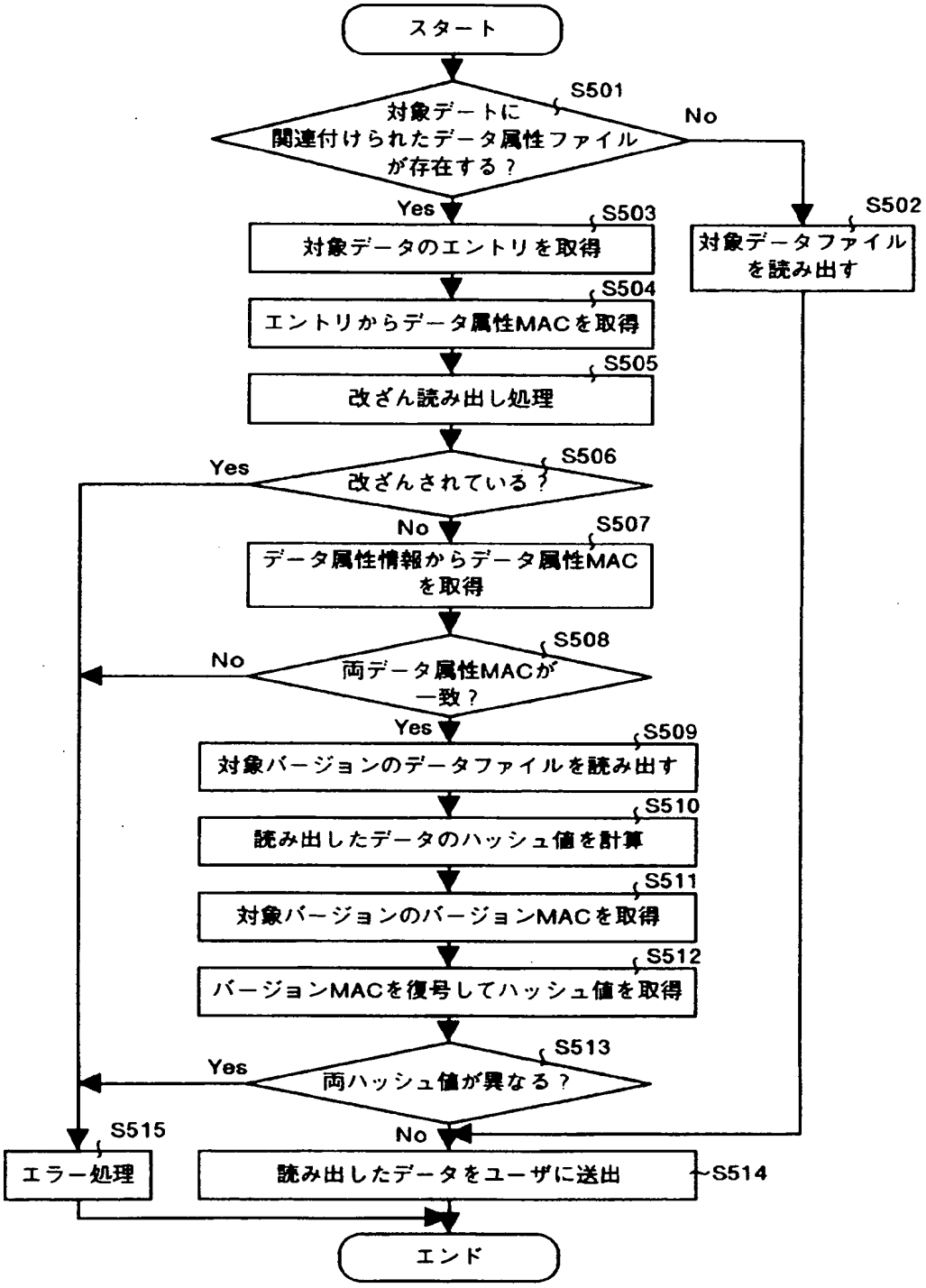
【図２】


スタート
S201
データ、データ属性コード、データ名を受け取る
S202
データ属性コードが「一般」である？
Yes
No
S203
受け取ったデータを受け取ったデータ名で保存
S204
初版としてバージョン属性情報を作成
S205
データ属性情報を作成
S206
保存データリストファイルを改ざん検知読み出し処理
S207
保存データリストに新しいデータのエントリを追加
S208
データをファイル保存
S209
データ属性情報を改ざん検知保存処理
S210
新しい保存データリストファイルを改ざん検知保存処理
S211
媒体認証コードリストを更新
エンド

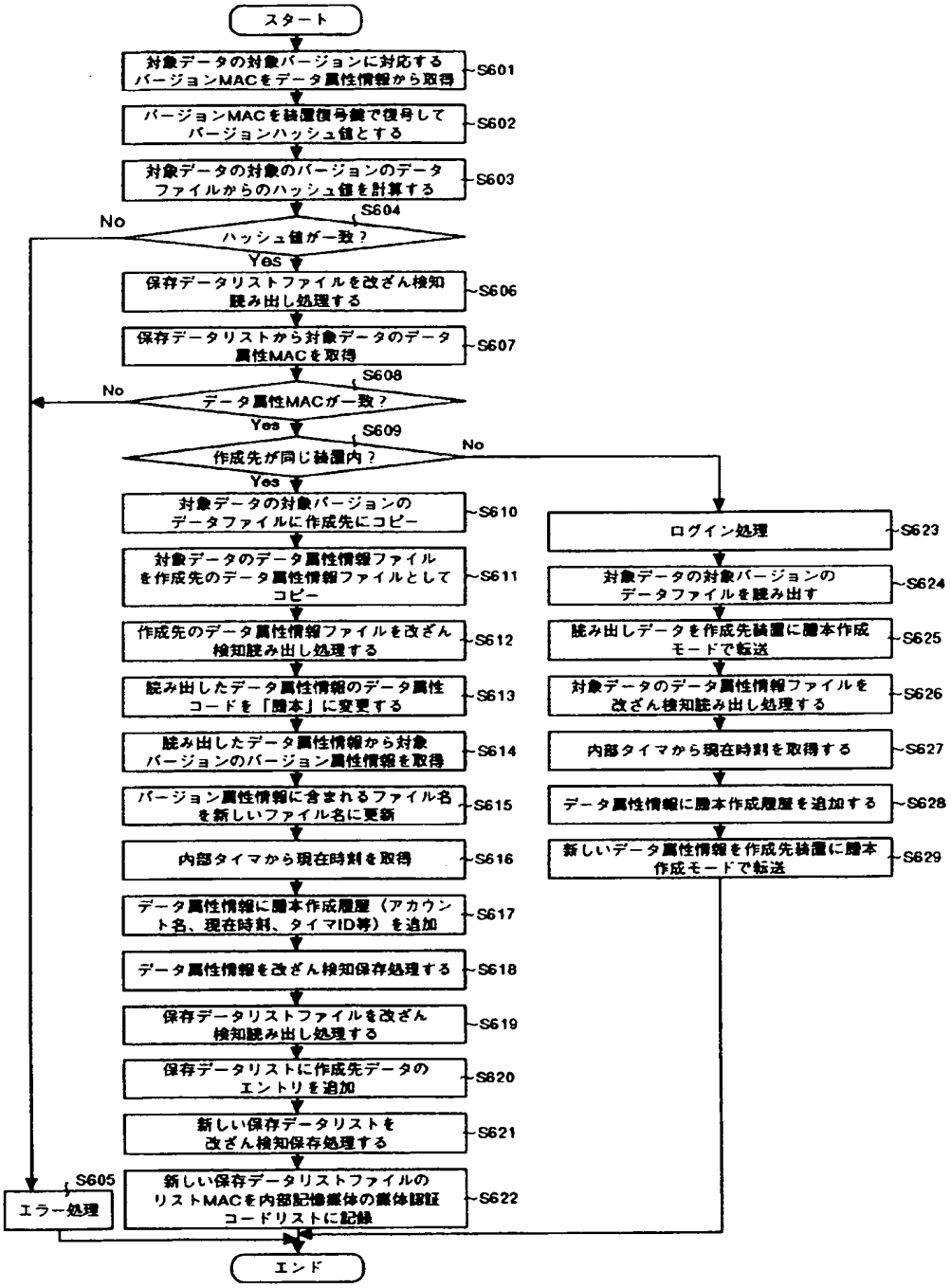
【図３】


データ
データ属性コード：「原本」
データ名：FileA.doc
新規保存
～S201
原本性保証
電子保存装置
S100
データ
バージョン属性
情報作成 ～S204
内部記憶媒体
媒体認証コードリスト
ハッシュ
計算
ハッシュ値
Ver.1
1999.3.27
FileA_1.doc
56KB
MAC
装置暗号鍵
で暗号化
MAC
バージョン属性MAC
装置暗号鍵
装置復号鍵
最新データ
識別番号
媒体識別番号
リストMAC
参照
更新 ～S211
データ属性
情報作成 ～S205
ハッシュ計算
R00012321
原本
1999.3.27
1999.3.27
ハッシュ値
装置暗号鍵
で暗号化
MAC
MAC
データ属性
MAC
保存データリスト
R00000001 原本 File01.doc 1999.3.21 1999.3.22 MAC
R00000002 原本 File02.doc 1999.3.22 1999.3.22 MAC
・・・
R00012321 原本 FileA.doc 1999.3.27 1999.3.27 MAC
MAC
エントリ
追加～S207
ハッシュ計算
ハッシュ値
装置暗号鍵で
暗号化
MAC
リストMAC
記録
記録
記録
大容量
記憶媒体
データ
ファイル
データ属性情報
ファイル
媒体識別番号
R11230089
データ
データ
属性情報
保存データリストファイル
保存データリスト
FileA_1.doc
FileA.doc.dat
R11230089.list

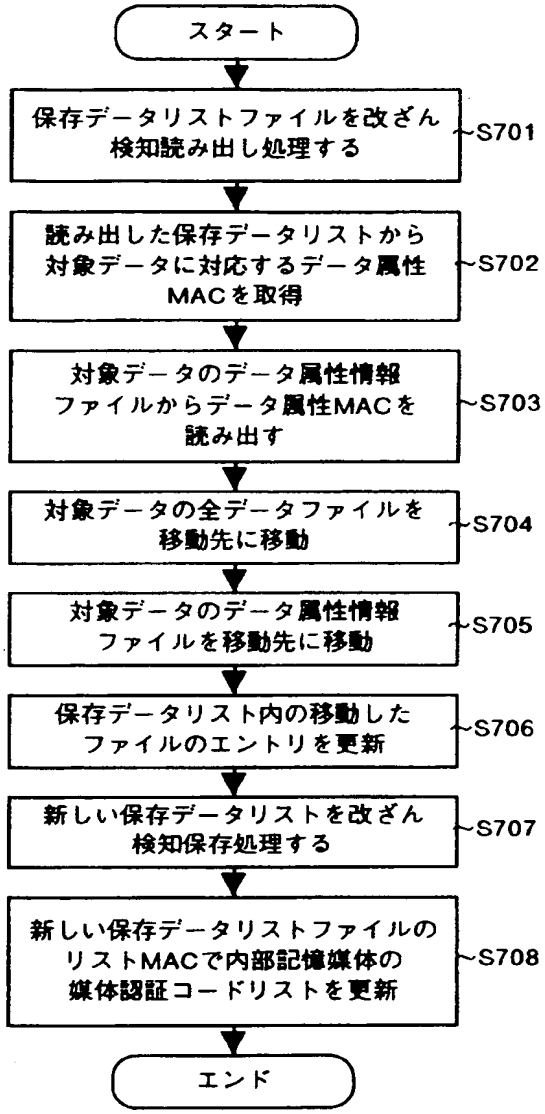
【図５】


スタート
S501
対象データに関連付けられたデータ属性ファイルが存在する？
No
Yes
S503
対象データのエントリを取得
S502
対象データファイルを読み出す
S504
エントリからデータ属性MACを取得
S505
改ざん読み出し処理
S506
Yes
改ざんされている？
No
S507
データ属性情報からデータ属性MACを取得
S508
No
両データ属性MACが一致？
Yes
S509
対象バージョンのデータファイルを読み出す
S510
読み出したデータのハッシュ値を計算
S511
対象バージョンのバージョンMACを取得
S512
バージョンMACを復号してハッシュ値を取得
S513
Yes
両ハッシュ値が異なる？
No
S515
エラー処理
S514
読み出したデータをユーザに送出
エンド

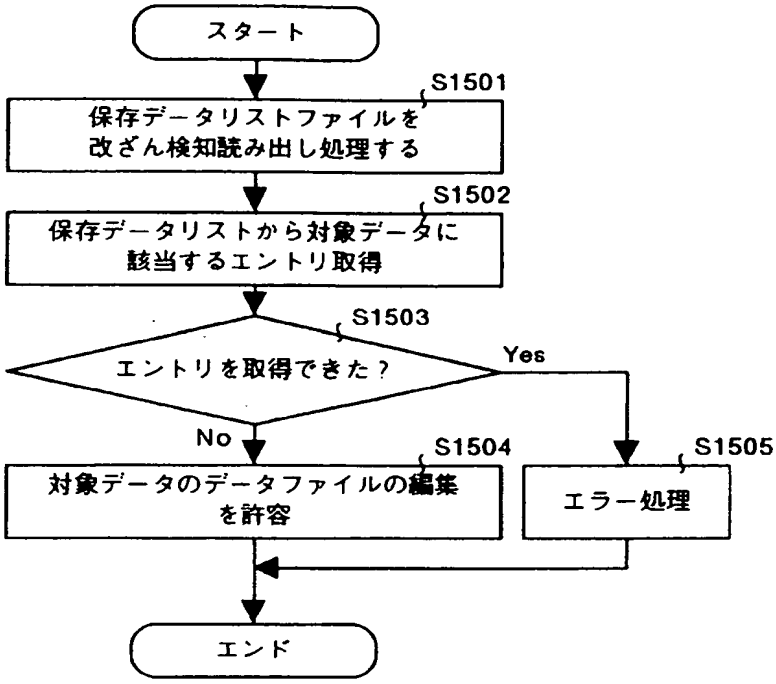
【図６】


スタート
対象データの対象バージョンに対応するバージョンMACをデータ属性情報から取得
S601
バージョンMACを装置復号鍵で復号してバージョンハッシュ値とする
S602
対象データの対象のバージョンのデータファイルからのハッシュ値を計算する
S603
S604
ハッシュ値が一致？
No
Yes
保存データリストファイルを改ざん検知読み出し処理する
S606
保存データリストから対象データのデータ属性MACを取得
S607
S608
データ属性MACが一致？
No
Yes
S609
作成先が同じ装置内？
No
Yes
対象データの対象バージョンのデータファイルに作成先にコピー
S610
対象データのデータ属性情報ファイルを作成先のデータ属性情報ファイルとしてコピー
S611
作成先のデータ属性情報ファイルを改ざん検知読み出し処理する
S612
読み出したデータ属性情報のデータ属性コードを「謄本」に変更する
S613
読み出したデータ属性情報から対象バージョンのバージョン属性情報を取得
S614
バージョン属性情報に含まれるファイル名を新しいファイル名に更新
S615
内部タイマから現在時刻を取得
S616
データ属性情報に謄本作成履歴（アカウント名、現在時刻、タイマID等）を追加
S617
データ属性情報を改ざん検知保存処理する
S618
保存データリストファイルを改ざん検知読み出し処理する
S619
保存データリストに作成先データのエントリを追加
S620
新しい保存データリストを改ざん検知保存処理する
S621
新しい保存データリストファイルのリストMACを内部記憶媒体の媒体認証コードリストに記録
S622
S605
エラー処理
ログイン処理
S623
対象データの対象バージョンのデータファイルを読み出す
S624
読み出しデータを作成先装置に謄本作成モードで転送
S625
対象データのデータ属性情報ファイルを改ざん検知読み出し処理する
S626
内部タイマから現在時刻を取得する
S627
データ属性情報に謄本作成履歴を追加する
S628
新しいデータ属性情報を作成先装置に謄本作成モードで転送
S629
エンド

【図７】



【図１５】



【図１７】

(a)

変更前	変更後
19990215 15：32：14 ID=1	19990215 15：30：00 ID=2
19990216 10：21：54 ID=2	19990116 10：22：00 ID=3
19990116 10：45：23 ID=3	19990216 10：46：00 ID=4

(b)

アクセス種別	アクセス日時	装置ＩＤ
CREATE	19990215 18：23：10 ID=1	R010-0001032
APPEND	19990215 18：23：30 ID=1	R010-0001032
MOVE TO	19990217 10：10：21 ID=3	R010-0001032
MOVE FROM	19990217 10：13：43 ID=2	R010-0001055

【図１９】

(a)

認証コードエントリ＃1	媒体識別番号
	メッセージ認識子（リストMAC）
認証コードエントリ＃2	
認証コードエントリ＃3	
…	
認証コードエントリ＃N	

(b)

アカウントエントリ＃1	アカウント名
	パスワード
アカウントエントリ＃2	
アカウントエントリ＃3	
…	
アカウントエントリ＃N	

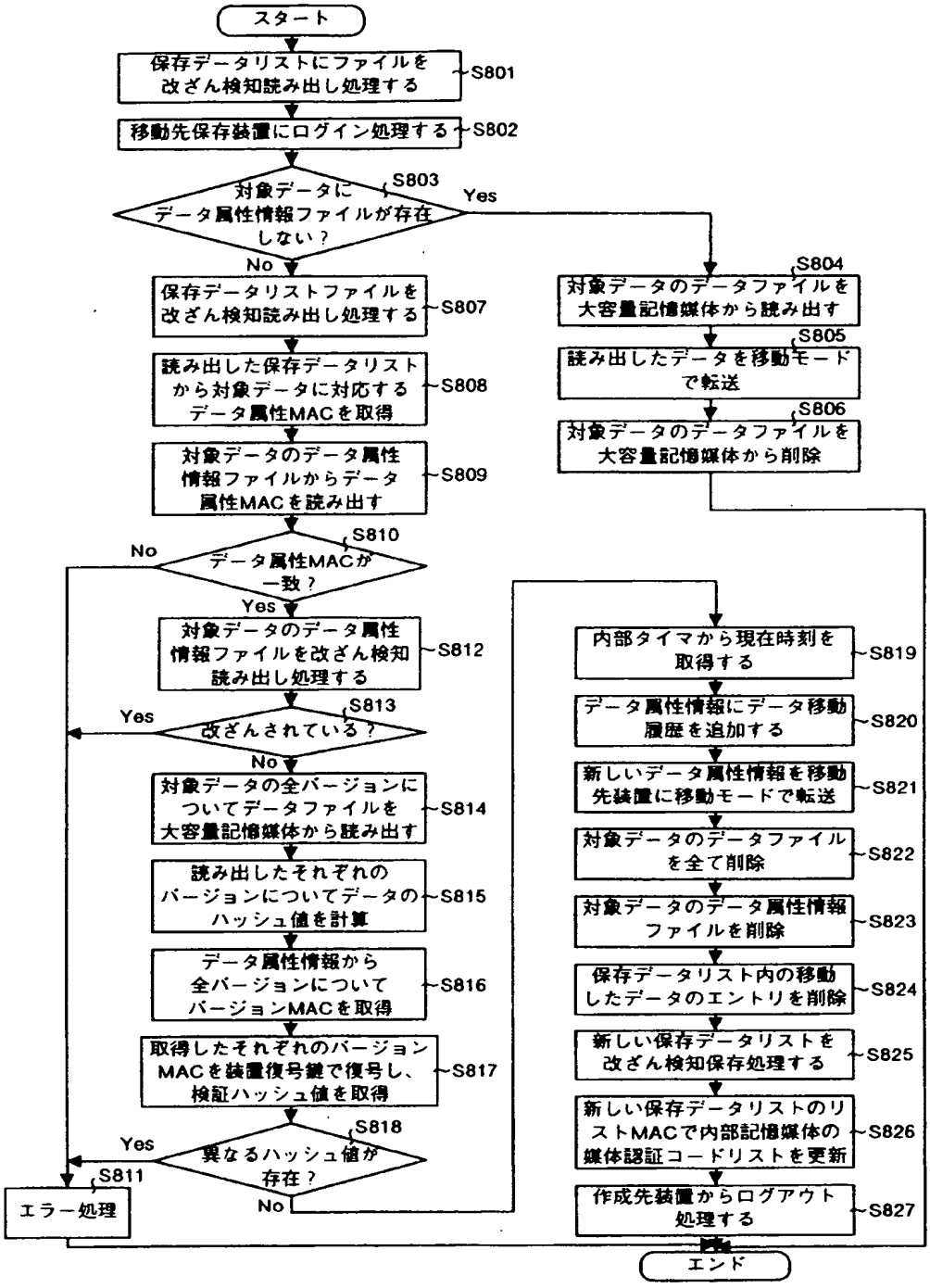
(c)

年
月
日
時
分
秒
タイマID

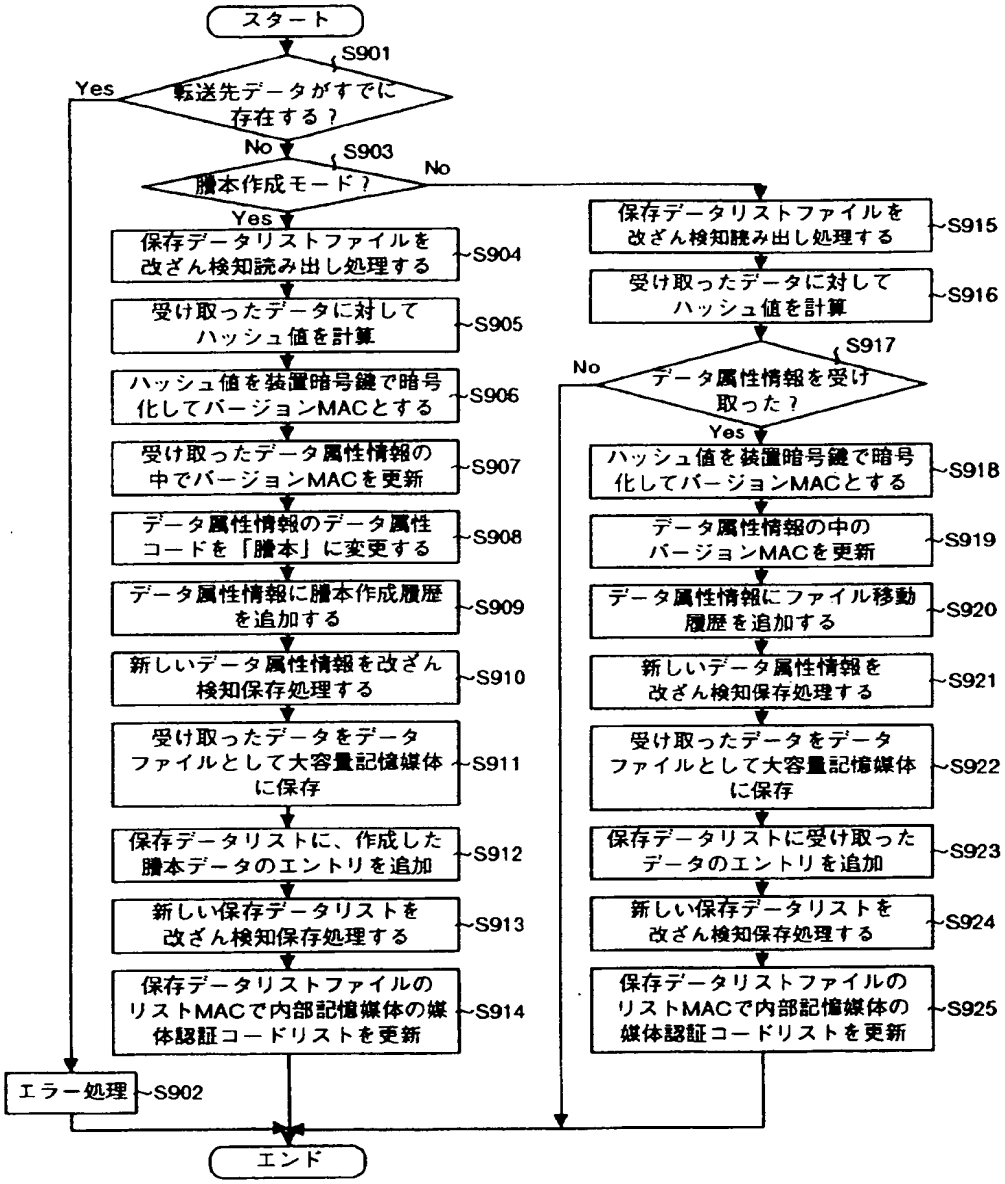
(d)

タイマ設定履歴＃1	設定前の日時情報
	設定後の日時情報
	アカウント名
タイマ設定履歴＃2	
タイマ設定履歴＃3	
…	

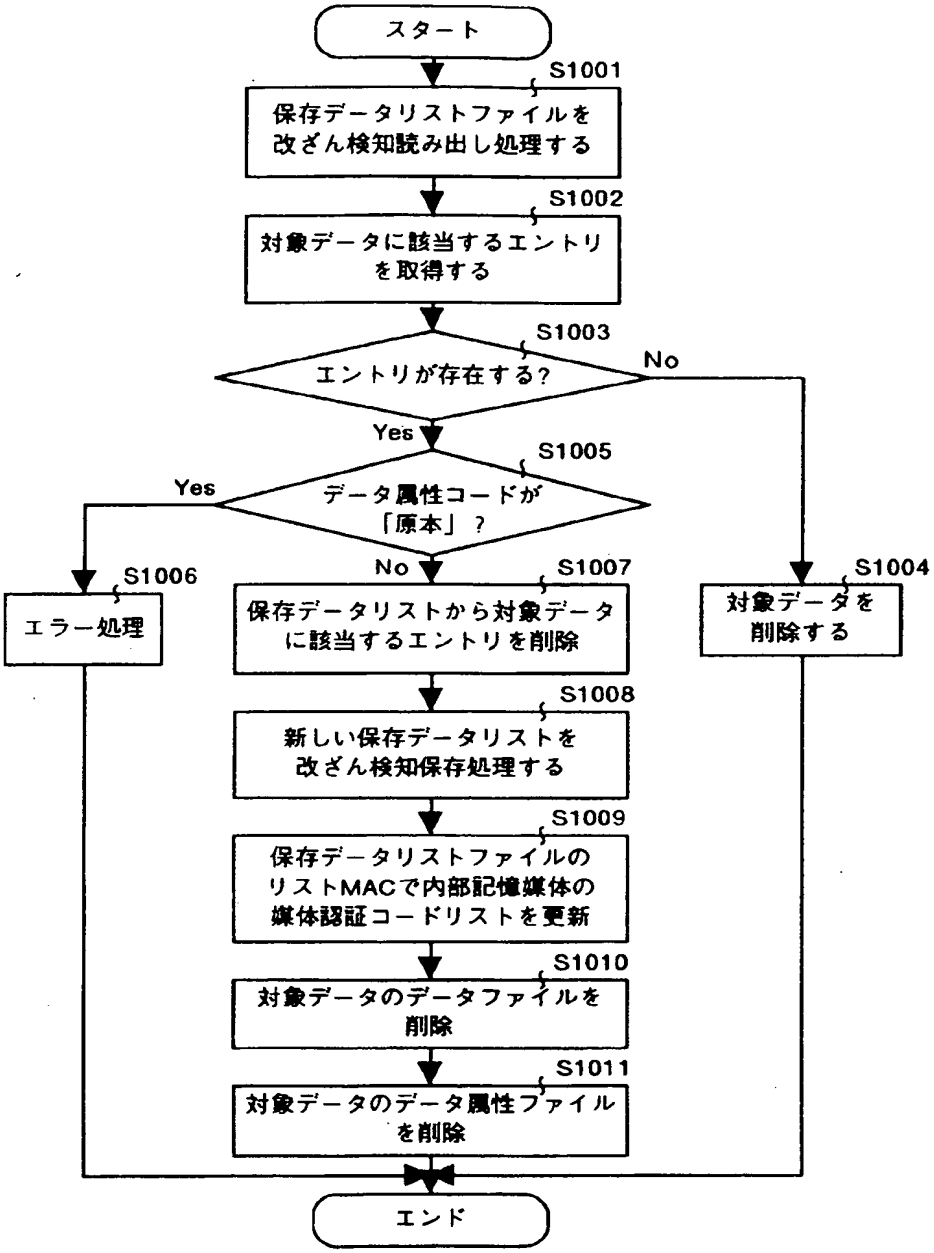
【図８】


スタート
保存データリストにファイルを改ざん検知読み出し処理する
S801
移動先保存装置にログイン処理する
S802
対象データにデータ属性情報ファイルが存在しない？
S803
Yes
No
保存データリストファイルを改ざん検知読み出し処理する
S807
読み出した保存データリストから対象データに対応するデータ属性MACを取得
S808
対象データのデータ属性情報ファイルからデータ属性MACを読み出す
S809
データ属性MACが一致？
S810
No
Yes
対象データのデータ属性情報ファイルを改ざん検知読み出し処理する
S812
改ざんされている？
S813
Yes
No
対象データの全バージョンについてデータファイルを大容量記憶媒体から読み出す
S814
読み出したそれぞれのバージョンについてデータのハッシュ値を計算
S815
データ属性情報から全バージョンについてバージョンMACを取得
S816
取得したそれぞれのバージョンMACを装置復号鍵で復号し、検証ハッシュ値を取得
S817
異なるハッシュ値が存在？
S818
Yes
No
エラー処理
S811
対象データのデータファイルを大容量記憶媒体から読み出す
S804
読み出したデータを移動モードで転送
S805
対象データのデータファイルを大容量記憶媒体から削除
S806
内部タイマから現在時刻を取得する
S819
データ属性情報にデータ移動履歴を追加する
S820
新しいデータ属性情報を移動先装置に移動モードで転送
S821
対象データのデータファイルを全て削除
S822
対象データのデータ属性情報ファイルを削除
S823
保存データリスト内の移動したデータのエントリを削除
S824
新しい保存データリストを改ざん検知保存処理する
S825
新しい保存データリストのリストMACで内部記憶媒体の媒体認証コードリストを更新
S826
作成先装置からログアウト処理する
S827
エンド

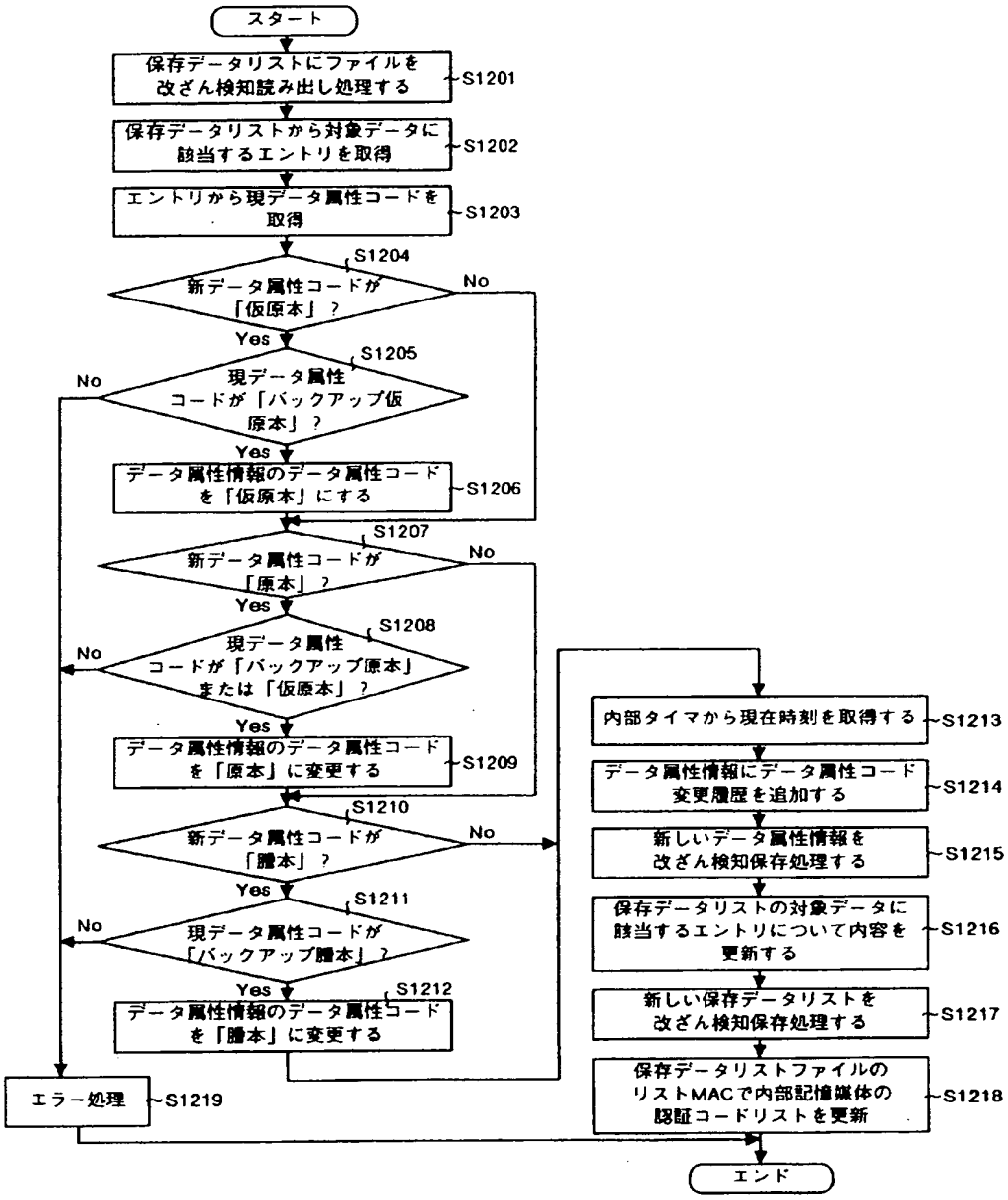
【図９】


スタート
S901
転送先データがすでに存在する？
Yes
No
S903
謄本作成モード？
No
Yes
保存データリストファイルを改ざん検知読み出し処理する
S904
受け取ったデータに対してハッシュ値を計算
S905
ハッシュ値を装置暗号鍵で暗号化してバージョンMACとする
S906
受け取ったデータ属性情報の中でバージョンMACを更新
S907
データ属性情報のデータ属性コードを「謄本」に変更する
S908
データ属性情報に謄本作成履歴を追加する
S909
新しいデータ属性情報を改ざん検知保存処理する
S910
受け取ったデータをデータファイルとして大容量記憶媒体に保存
S911
保存データリストに、作成した謄本データのエントリを追加
S912
新しい保存データリストを改ざん検知保存処理する
S913
保存データリストファイルのリストMACで内部記憶媒体の媒体認証コードリストを更新
S914
エラー処理
S902
保存データリストファイルを改ざん検知読み出し処理する
S915
受け取ったデータに対してハッシュ値を計算
S916
S917
データ属性情報を受け取った？
No
Yes
ハッシュ値を装置暗号鍵で暗号化してバージョンMACとする
S918
データ属性情報の中のバージョンMACを更新
S919
データ属性情報にファイル移動履歴を追加する
S920
新しいデータ属性情報を改ざん検知保存処理する
S921
受け取ったデータをデータファイルとして大容量記憶媒体に保存
S922
保存データリストに受け取ったデータのエントリを追加
S923
新しい保存データリストを改ざん検知保存処理する
S924
保存データリストファイルのリストMACで内部記憶媒体の媒体認証コードリストを更新
S925
エンド

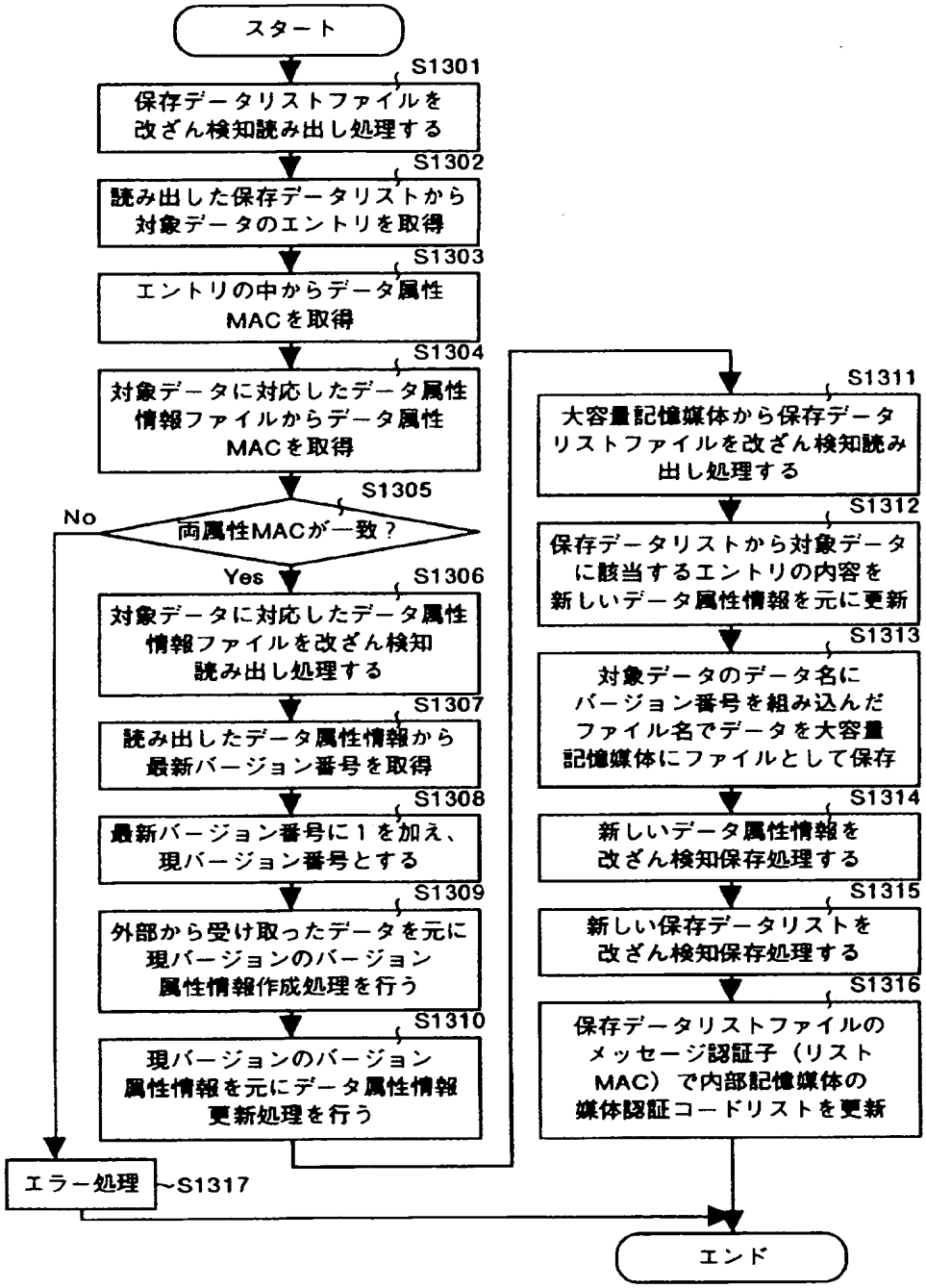
【図１０】


スタート
S1001
保存データリストファイルを改ざん検知読み出し処理する
S1002
対象データに該当するエントリを取得する
S1003
エントリが存在する?
No
Yes
S1005
データ属性コードが「原本」?
Yes
No
S1006
エラー処理
S1007
保存データリストから対象データに該当するエントリを削除
S1004
対象データを削除する
S1008
新しい保存データリストを改ざん検知保存処理する
S1009
保存データリストファイルのリストMACで内部記憶媒体の媒体認証コードリストを更新
S1010
対象データのデータファイルを削除
S1011
対象データのデータ属性ファイルを削除
エンド

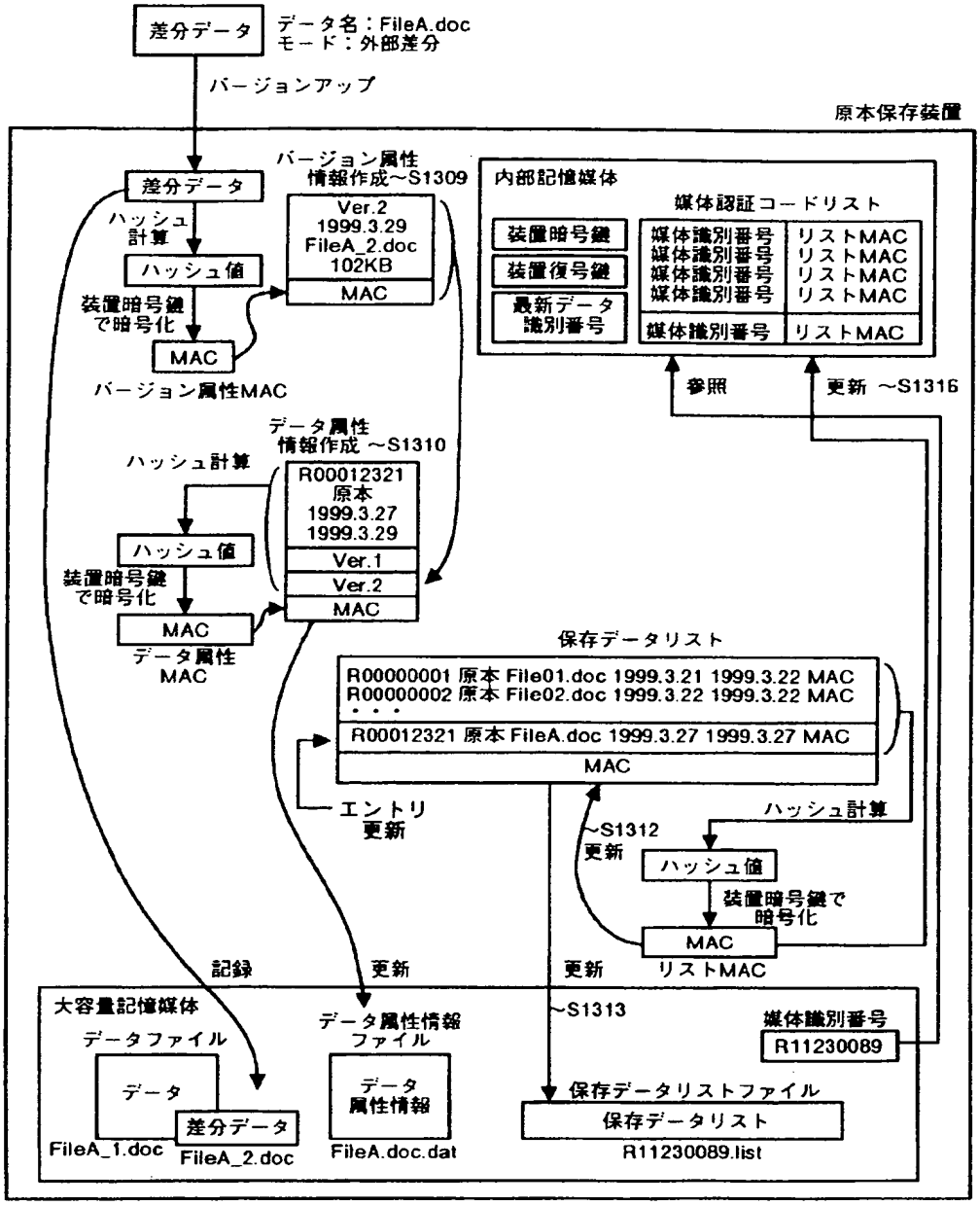
【図１２】


スタート
保存データリストにファイルを改ざん検知読み出し処理する
S1201
保存データリストから対象データに該当するエントリを取得
S1202
エントリから現データ属性コードを取得
S1203
S1204
新データ属性コードが「仮原本」？
No
Yes
S1205
現データ属性コードが「バックアップ仮原本」？
No
Yes
データ属性情報のデータ属性コードを「仮原本」にする
S1206
S1207
新データ属性コードが「原本」？
No
Yes
S1208
現データ属性コードが「バックアップ原本」または「仮原本」？
No
Yes
データ属性情報のデータ属性コードを「原本」に変更する
S1209
S1210
新データ属性コードが「謄本」？
No
Yes
S1211
現データ属性コードが「バックアップ謄本」？
No
Yes
データ属性情報のデータ属性コードを「謄本」に変更する
S1212
エラー処理
S1219
内部タイマから現在時刻を取得する
S1213
データ属性情報にデータ属性コード変更履歴を追加する
S1214
新しいデータ属性情報を改ざん検知保存処理する
S1215
保存データリストの対象データに該当するエントリについて内容を更新する
S1216
新しい保存データリストを改ざん検知保存処理する
S1217
保存データリストファイルのリストMACで内部記憶媒体の認証コードリストを更新
S1218
エンド

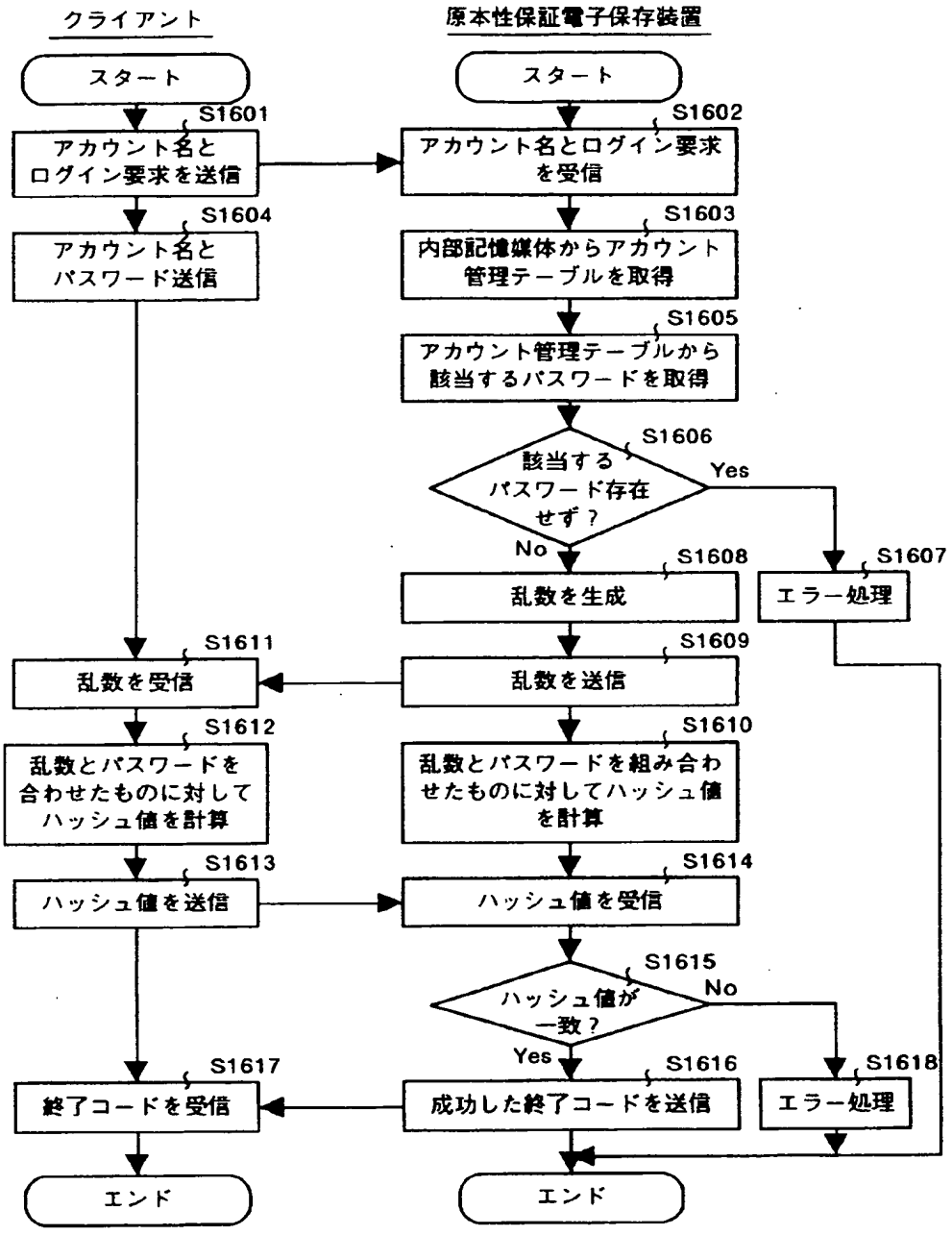
【図１３】


スタート
S1301
保存データリストファイルを改ざん検知読み出し処理する
S1302
読み出した保存データリストから対象データのエントリを取得
S1303
エントリの中からデータ属性MACを取得
S1304
対象データに対応したデータ属性情報ファイルからデータ属性MACを取得
S1305
両属性MACが一致？
No
Yes
S1306
対象データに対応したデータ属性情報ファイルを改ざん検知読み出し処理する
S1307
読み出したデータ属性情報から最新バージョン番号を取得
S1308
最新バージョン番号に１を加え、現バージョン番号とする
S1309
外部から受け取ったデータを元に現バージョンのバージョン属性情報作成処理を行う
S1310
現バージョンのバージョン属性情報を元にデータ属性情報更新処理を行う
エラー処理
S1317
S1311
大容量記憶媒体から保存データリストファイルを改ざん検知読み出し処理する
S1312
保存データリストから対象データに該当するエントリの内容を新しいデータ属性情報を元に更新
S1313
対象データのデータ名にバージョン番号を組み込んだファイル名でデータを大容量記憶媒体にファイルとして保存
S1314
新しいデータ属性情報を改ざん検知保存処理する
S1315
新しい保存データリストを改ざん検知保存処理する
S1316
保存データリストファイルのメッセージ認証子（リストMAC）で内部記憶媒体の媒体認証コードリストを更新
エンド

【図１４】


差分データ
データ名：FileA.doc
モード：外部差分
バージョンアップ
原本保存装置
差分データ
バージョン属性
情報作成～S1309
Ver.2
1999.3.29
FileA_2.doc
102KB
MAC
ハッシュ
計算
ハッシュ値
装置暗号鍵
で暗号化
MAC
バージョン属性MAC
内部記憶媒体
媒体認証コードリスト
装置暗号鍵
装置復号鍵
最新データ
識別番号
媒体識別番号
リストMAC
参照
更新 ～S1316
データ属性
情報作成 ～S1310
ハッシュ計算
R00012321
原本
1999.3.27
1999.3.29
Ver.1
Ver.2
MAC
ハッシュ値
装置暗号鍵
で暗号化
MAC
データ属性
MAC
保存データリスト
R00000001 原本 File01.doc 1999.3.21 1999.3.22 MAC
R00000002 原本 File02.doc 1999.3.22 1999.3.22 MAC
・・・
R00012321 原本 FileA.doc 1999.3.27 1999.3.27 MAC
MAC
エントリ
更新
～S1312
更新
ハッシュ計算
ハッシュ値
装置暗号鍵で
暗号化
MAC
リストMAC
記録
更新
更新
～S1313
大容量記憶媒体
データファイル
データ
差分データ
FileA_1.doc
FileA_2.doc
データ属性情報
ファイル
データ
属性情報
FileA.doc.dat
媒体識別番号
R11230089
保存データリストファイル
保存データリスト
R11230089.list

【図１６】


クライアント
原本性保証電子保存装置
スタート
スタート
S1601
アカウント名と
ログイン要求を送信
S1602
アカウント名とログイン要求
を受信
S1604
アカウント名と
パスワード送信
S1603
内部記憶媒体からアカウント
管理テーブルを取得
S1605
アカウント管理テーブルから
該当するパスワードを取得
S1606
該当する
パスワード存在
せず？
Yes
No
S1608
乱数を生成
S1607
エラー処理
S1611
乱数を受信
S1609
乱数を送信
S1612
乱数とパスワードを
合わせたものに対して
ハッシュ値を計算
S1610
乱数とパスワードを組み合わ
せたものに対してハッシュ値
を計算
S1613
ハッシュ値を送信
S1614
ハッシュ値を受信
S1615
ハッシュ値が
一致？
No
Yes
S1617
終了コードを受信
S1616
成功した終了コードを送信
S1618
エラー処理
エンド
エンド

【図１８】

(a)

メッセージ認証子（リストMAC）	
リストエントリ＃１	データ認識番号
	データ名
	フルパス名
	属性コード
	作成日時情報
	更新日時情報
	原本化日時情報
	メッセージ認証子（データ属性MAC）
リストエントリ＃２	
リストエントリ＃３	
…	

(b)

メッセージ認証子（リストMAC）	
属性管理データ	データ認識番号
	データ名
	データ属性コード（原本、謄本、仮原本）
	作成日時情報
	最終更新日時情報
	最新バージョン番号
	バージョン属性情報＃１
	バージョン属性情報＃２
	…
	バージョン属性情報＃Ｎ

(c)

メッセージ認証子（バージョン属性MAC）	
バージョン管理データ	バージョン番号
	データ属性コード（原本、謄本、仮原本）
	作成日時情報
	最終更新日時情報
	データファイルタイプ（完全、外部差分）
	データファイル名
	データファイルサイズ
アクセス履歴＃１	アカウント名
	アクセス日時情報
	アクセス種別（作成、原本化、参照）
	保存装置識別番号
アクセス履歴＃２	
アクセス履歴＃３	
…	
アクセス履歴＃Ｎ	

フロントページの続き

Ｆターム(参考) 5B017 AA01 AA06 BA05 BA06 BA07
BB02 BB10 CA09 CA16
5J104 AA08 NA02 NA06 NA27 PA14
9A001 BB01 BB03 BB04 CC08 EE03
GG22 LL02 LL03